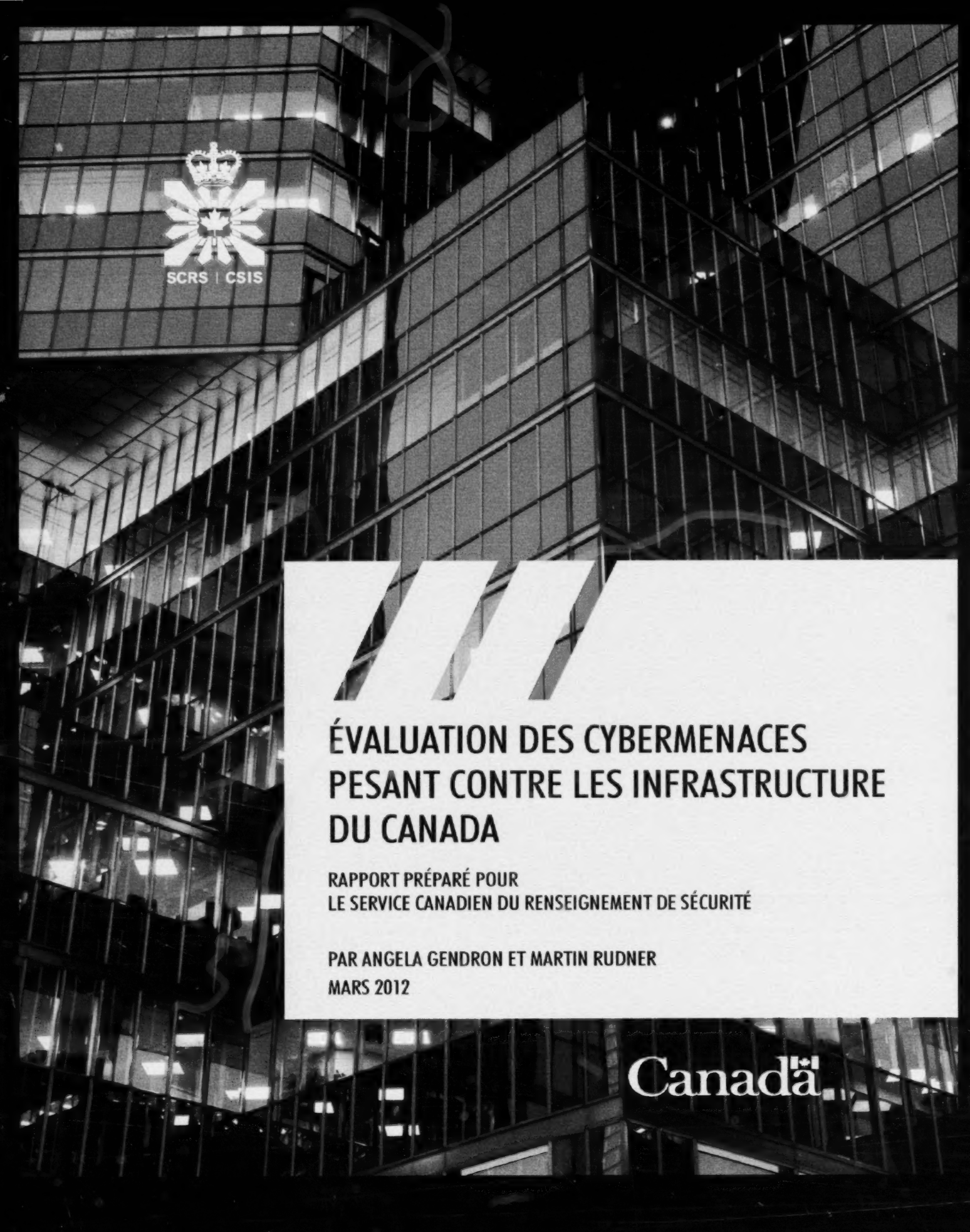


# ÉVALUATION DES CYBERMENACES PESANT CONTRE LES INFRASTRUCTURE DU CANADA

RAPPORT PRÉPARÉ POUR
LE SERVICE CANADIEN DU RENSEIGNEMENT DE SÉCURITÉ

PAR ANGELA GENDRON ET MARTIN RUDNER

MARS 2012

Canada

Pensez à recycler

Ce document est imprimé avec de l'encre sans danger pour l'environnement

FSC

BY NC ND

*Études hors-série* 2012-10-01

Cette étude a été réalisée à la demande du Service canadien du renseignement de securité (SCRS). Les idées qui y sont exprimées sont celles des auteurs et ne représentent pas la position officielle du SCRS.

*Crédit photo : istockphoto.com*

# ÉVALUATION DES CYBERMENACES PESANT CONTRE LES INFRASTRUCTURES DU CANADA

RAPPORT PRÉPARÉ POUR
LE SERVICE CANADIEN DU RENSEIGNEMENT DE SÉCURITÉ

PAR ANGELA GENDRON ET MARTIN RUDNER

MARS 2012

# TABLE DES MATIÈRES


**SOMMAIRE** 5

**CHAPITRE 1 – INFRASTRUCTURE CANADIENNE ET INTERDÉPENDANCES** 13

Contexte 13
Dynamiques structurelles des secteurs des infrastructures essentielles au Canada 16
Énergie et services publics 16
Transport 18
Finances 18
Technologies de l'information et de la communication (TIC) 19
Infrastructures et interdépendances 20

**CHAPITRE 2 – CONTEXTE DE LA MENACE CYBERNÉTIQUE** 25

Terrorisme international 26
Actes de terrorisme, d'espionnage et de sabotage parrainés des États 30
Hacktivisme malveillant 36
Menaces internes 40

**CHAPITRE 3 – RISQUES ET PROBABILITÉS QUE DES CYBERATTAQUES SOIENT LANCÉES** 43

Le cyberspace – caractéristiques et préoccupations 43
Nouvelles menaces 47
Évaluer les risques et les vulnérabilités 49

**CHAPITRE 4 – CONTRER LES CYBERMENACES – UNE APPROCHE DE PARTENARIAT EN MATIÈRE DE PROTECTION DES INFRASTRUCTURES ESSENTIELLES** 51

ALLER DE L'AVANT : LE RÔLE DU RENSEIGNEMENT 55

ANNEXE A 61
DYNAMIQUES STRUCTURELLES DU SECTEUR DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

ANNEXE B 65
MODÉLISATION DES RISQUES ET DES VULNÉRABILITÉS

NOTES EN FIN D'OUVRAGE 67

# ÉVALUATION DES CYBERMENACES PESANT CONTRE LES INFRASTRUCTURES DU CANADA

## SOMMAIRE

La présente étude comporte trois objectifs : 1) examiner l'environnement de la cybermenace qui pèse contre les infrastructures essentielles du Canada, en misant plus précisément sur les quatre principaux secteurs (énergie et services publics, transport, finances et technologies de l'information et de la communication), et leurs interdépendances, 2) déterminer les entités qui ont la capacité et la motivation politique et idéologique de lancer des cyberattaques contre les infrastructures essentielles de notre pays et de menacer nos intérêts nationaux et 3) discuter du rôle du renseignement en matière de lutte contre ces menaces. Les cyberactivités des criminels et des gangs du crime organisé qui sont motivés par un profit financier ou matériel sont exclues de la présente étude.

## CONTEXTE

Les menaces pesant contre les infrastructures essentielles ont été jugées comme une préoccupation nationale en matière de sécurité dans la politique canadienne de sécurité nationale intitulée « Protéger une société ouverte » (2004). La Stratégie nationale sur les infrastructures essentielles (2010) a ensuite divisé les infrastructures essentielles en secteurs qui ont en commun un élément informatisé duquel dépendent les systèmes physiques. Ces secteurs sont devenus sans cesse plus interconnectés et interdépendants, ce qui les rend plus vulnérables aux cybermenaces et qui fait d'eux une cible plus attrayante. Une cyberattaque pourrait causer des dommages étendus aux réseaux numériques ainsi que des interruptions et des perturbations physiques.

La responsabilité de la protection des biens essentiels incombe d'abord aux propriétaires et aux exploitants. Toutefois, compte tenu des interdépendances au sein des secteurs des infrastructures et entre ceux-ci, seul un partenariat entre les secteurs public et privé mobilisant tous les intervenants permettra de combattre efficacement les menaces, d'atténuer les conséquences et d'accroître la résilience. Des réseaux d'échange d'information à l'échelle nationale propres à chacun des secteurs ont été établis.

La responsabilité de la protection des biens essentiels incombe d'abord aux propriétaires et aux exploitants. Toutefois, compte tenu des interdépendances au sein des secteurs des infrastructures et entre ceux-ci, seul un partenariat entre les secteurs public et privé mobilisant tous les intervenants permettra de combattre efficacement les menaces, d'atténuer les conséquences et d'accroître la résilience. Des réseaux d'échange d'information à l'échelle nationale propres à chacun des secteurs ont été établis.

## DYNAMIQUES STRUCTURELLES DES SECTEURS DES INFRASTRUCTURES ESSENTIELLES AU CANADA

La caractéristique déterminante d'une société moderne axée sur les connaissances et de son économie est leur dépendance aux technologies de l'information et de la communication (TIC). Les quatre secteurs abordés dans le présent rapport évoluent dans un environnement économique concurrentiel à l'échelle mondiale dans lequel de telles technologies sont de plus en plus utilisées pour favoriser les économies et l'efficacité opérationnelle. Les produits et services de chacun de ces secteurs sont importants pour le bien-être et la prospérité des Canadiens et contribuent de manière considérable au produit intérieur brut du Canada. En outre, le secteur canadien de l'énergie est étroitement intégré aux États-Unis à l'échelle du continent. Par conséquent, une interruption majeure de l'approvisionnement aurait des répercussions profondes non seulement sur les consommateurs canadiens, mais aussi sur les marchés d'exportation aux États-Unis.

De nouvelles technologies, comme les systèmes de contrôle informatisés, sont utilisées dans bon nombre d'industries et d'infrastructures essentielles du Canada pour surveiller et contrôler les processus délicats et les fonctions physiques. Cette connectivité accrue, jumelée à l'insécurité inhérente aux connexions Internet, a fait augmenter les risques de cyberattaques.

## INFRASTRUCTURES ET INTERDÉPENDANCES

Il y a des interdépendances lorsque les producteurs et fournisseurs de produits et services, *au sein* des secteurs des infrastructures essentielles et *entre* ceux-ci, deviennent mutuellement dépendants, parfois dans une mesure différente et inégale. Par le passé, la dépendance découlait de relations physiques ou

géographiques. Le développement du cyberespace a entraîné l'établissement de nouvelles relations, qui créent davantage de vulnérabilités.

Les systèmes de communication de données connectés à Internet et les méthodes informatisées de commande et de contrôle automatisés par des moyens électroniques à distance sont répandus au sein des infrastructures essentielles du Canada. Ces systèmes et méthodes permettent une surveillance et un contrôle centralisés de la production et des processus de prestation de services dans des établissements précis et des infrastructures interdépendantes au sein de vastes régions géographiques. L'augmentation de la connectivité signifie que la défaillance de l'une des composantes essentielles est susceptible d'avoir des répercussions d'une portée considérable. Des perturbations liées à la disponibilité des produits et services pourraient avoir des conséquences graves sur le secteur commercial et la société, ce qui se répercutera non seulement dans les secteurs, mais aussi dans les administrations fédérale, provinciales et territoriales, ainsi que les secteurs privé et public.

La complexité de ces liens fait en sorte que les propriétaires et exploitants ont beaucoup de difficultés à avoir une « connaissance de la situation » suffisante. Pour réduire les risques découlant des interdépendances, il faudra adopter une approche de collaboration entre les secteurs privé et public.

## ENVIRONNEMENT DE LA CYBERMENACE

La dimension cybernétique a transformé les infrastructures économiques et les biens nationaux clés pour faire d'eux des cibles plus attrayantes et de grande valeur, tout en les rendant plus vulnérables aux menaces importantes. Dans un environnement asymétrique, le cyberespace fournit un havre relativement peu onéreux et sans risque à toutes sortes d'opérations perturbatrices et liées à la collecte du renseignement.

Les menaces majeures (qui peuvent être encouragées et aidées par l'ingérence étrangère ou des entités étatiques) découlent du terrorisme international, du sabotage et de l'espionnage parrainés par un État ainsi que de l'« hacktivisme » malveillant. Dans tous les cas, il est possible de recourir à un « agent interne » pour lancer l'attaque ou aider à le faire. À l'étape initiale, il n'est pas toujours possible de déterminer si un cyberincident est parrainé par un État, autonome ou perpétré par un groupe malveillant ou criminel.

a) Le terrorisme international, plus particulièrement l'extrémisme islamiste sunnite, a été jugé, dans la Stratégie antiterroriste du Canada, comme la principale menace à la sécurité nationale du Canada. Même si les secteurs de l'énergie, du transport et des finances ont longtemps été des cibles attrayantes pour les attaques physiques, on s'inquiète de plus en plus du fait que les islamistes se serviront d'Internet pour lancer des cyberattaques afin de promouvoir leur soi-disant djihad économique. Pour le moment, rien ne prouve la présence de cyberterrorisme systématique de la part du groupe al Qaïda ou de ses affiliés, mais celui-ci a plaidé explicitement en faveur d'un djihad cybernétique ainsi que d'autres activités terroristes, alors que d'autres érudits islamistes ont affirmé la légitimité religieuse du « djihad économique ».

b) Le terrorisme, l'espionnage et le sabotage parrainés par un État sont également une source de préoccupation : si les terroristes et les groupes terroristes réussissent à attirer des États parrains, la menace aux réseaux informatiques pourrait augmenter. Les « menaces persistantes avancées », qui sont les infections d'ordinateurs les plus importantes élaborées jusqu'à maintenant, exigent des niveaux de ressources techniques et financières que l'on a associés à ceux des États.

La dépendance du Canada aux réseaux numériques et aux communications par Internet, sa société ouverte et le caractère attrayant de ses industries avancées en tant que cibles pour le vol de propriété intellectuelle le rendent vulnérable aux activités de sabotage et d'espionnage cybernétiques. Bon nombre de ces cyberattaques sont sensément attribuables à des pirates informatiques de la Chine et de la Russie appuyés par le gouvernement. La dimension cybernétique a changé le caractère de l'espionnage, puisque les acteurs non étatiques et l'utilisation d'intermédiaires et de technologies cybernétiques rendent la détection et l'attribution difficiles.

c) La plupart des incidents liés au piratage informatique sont motivés par la criminalité, des protestations ou un défi technique. Toutefois, le piratage informatique commis par des activistes malveillants (ou hacktivistes), qui ciblent les systèmes d'exploitation contrôlés par ordinateur au sein des infrastructures essentielles, constitue une menace potentielle à la sécurité nationale. Les interruptions majeures de l'approvisionnement ou l'exposition de dossiers du gouvernement de nature délicate peuvent entraîner une souffrance humaine généralisée, voire la perte de la vie, ainsi que la perte de la confiance envers le gouvernement.

d) Les nouvelles cybertechnologies liées à l'agrégation, à la conservation et à la récupération de données ont contribué à accroître la menace provenant d'agents internes. Qu'ils soient lésés, subornés ou infiltrés, les agents internes impliqués dans des activités au sein d'industries primaires ou d'industries de fabrication de produits de haute technologie, du secteur de l'énergie et des services publics ou de ministères et organismes gouvernementaux sont devenus un sujet de préoccupation important. Le Department of Homeland Security (DHS) des États-Unis a avisé que les extrémistes violents ont obtenu des postes d'agents internes au sein du secteur de l'énergie et des services publics de ce pays et qu'ils posent une menace physique et cybernétique importante aux infrastructures essentielles.

## RISQUES ET PROBABILITÉS DE CYBERATTAQUES

Les techniques et les technologies en évolution rapide ont fait surgir de nouvelles menaces plus sophistiquées fondées sur l'amélioration des ensembles de compétences des attaquants et les technologies avancées qui sont à leur disposition. Par ailleurs, l'externalisation de la conception, de la mise en œuvre et du maintien des TIC dans tous les secteurs à des fournisseurs indépendants, notamment des pays en développement, des centres d'informatique en nuage et des grands centres de fusion de données, ainsi que l'utilisation de technologies commerciales grand public, ont augmenté les vulnérabilités et les risques.

La propagation de nouvelles cybermenaces, l'absence de limites géographiques et le problème de la détermination de l'attribution nuisent aux efforts de lutte contre les attaques aux systèmes d'information. Parmi les obstacles figurent non seulement les limites géographiques nationales relatives à l'échange d'information et à l'établissement de lois et de règlements, mais aussi la propriété fragmentée et le contrôle réglementaire de l'infrastructure des TIC, qui représentent un défi majeur à l'échelle mondiale.

L'adoption d'une méthode fiable d'estimation des risques associés aux infrastructures essentielles pourrait aider les gestionnaires à décider du niveau de sécurité requis dans un établissement particulier, mais la complexité structurelle et les obstacles en matière d'information nuisent aux efforts visant à effectuer des évaluations réalistes des menaces et des vulnérabilités. Certaines méthodologies d'analyse des risques les plus récentes tentent d'intégrer les « risques pernicieux » (ceux qui comme le terrorisme ne peuvent pas être déterminés par des méthodes actuarielles conventionnelles) à des évaluations de la probabilité.

## LUTTER CONTRE LA MENACE : UNE APPROCHE DE PARTENARIAT EN MATIÈRE DE PROTECTION DES INFRASTRUCTURES

Les mesures de défense actuelles ne suffiront pas à assurer l'intégrité et l'accessibilité des systèmes d'information canadiens ou à empêcher les infrastructures essentielles d'être perturbées ou endommagées. Si la sécurité de l'information est perçue comme un problème purement technique, les efforts visant à l'améliorer produiront des solutions d'ingénierie, surtout dans le secteur privé. L'adoption d'une stratégie nationale plus holistique permettrait toutefois de considérer la question sur le plan de la ***protection d'une société axée sur l'information dans son ensemble***, plutôt que la protection des infrastructures liées à l'information. Cette approche exige que les services du renseignement adoptent une approche proactive en matière de cybersécurité fondée sur la ***prévention*** des infections, plutôt qu'une approche qui ne fait que réagir à celles-ci. Cette nouvelle approche permettrait également de mettre davantage l'accent sur la lutte contre les activités cybernétiques qui ciblent les secrets du gouvernement et des entreprises, ce qui représente une menace aussi importante à la sécurité nationale que les cyberattaques d'envergure visant à endommager ou à perturber les systèmes informatiques.

Les propriétaires et exploitants des infrastructures essentielles ont la responsabilité première de protéger leurs biens, mais la sécurité nationale est une responsabilité qui incombe à l'État; la protection des biens essentiels contre les cybermenaces qui ont des répercussions sur la sécurité nationale requiert un partenariat entre tous les intervenants. Ceux-ci pourraient également être appelés à tenir compte de la façon dont les coûts financiers associés à la protection des infrastructures essentielles pourraient être partagés entre les intervenants qui en bénéficient.

## VOIE À SUIVRE

Le renseignement est un élément clé de la prise de décisions tactiques et stratégiques. Dans le domaine cybernétique, le renseignement permet d'accroître la capacité des gouvernements et des intervenants à détecter les menaces, à évaluer les cybercapacités des adversaires, à évaluer les répercussions de cyberattaques, à atténuer les risques et à faire de la cybersécurité un processus plus efficace et plus rentable grâce à des décisions éclairées. L'objectif doit être

de s'assurer que les coûts engagés par les adversaires qui tentent de tirer profit des vulnérabilités soient élevés, que les perspectives de réussite soient minimes et que l'industrie et la société soient adéquatement préparées à faire preuve de résilience.

La nouvelle stratégie de lutte contre le terrorisme du Canada appuie explicitement des mesures proactives d'application de la loi et de renseignements pour faire du Canada une cible plus difficile pour les terroristes. La lutte contre les cybermenaces aux infrastructures essentielles exige une approche qui va au delà de la simple défense et des solutions techniques et qui intègre les capacités et les biens du Canada en matière de renseignements (y compris le renseignement d'origine électromagnétique) aux défis liés à la détection et à la prévention des attaques prospectives.

# ÉVALUATION DES CYBERMENACES PESANT CONTRE LES INFRASTRUCTURES DU CANADA

## CHAPITRE 1
## INFRASTRUCTURE CANADIENNE ET INTERDÉPENDANCES

La présente étude examine l'environnement de la cybermenace qui pèse contre les infrastructures essentielles du Canada, en misant plus précisément sur les quatre principaux secteurs (énergie et services publics, transport, finances et technologies de l'information et de la communication), et leurs interdépendances. Elle détermine les entités qui ont la capacité et la motivation politique et idéologique de lancer des cyberattaques contre les infrastructures essentielles de notre pays et de menacer nos intérêts nationaux. Enfin, elle discute du rôle du renseignement en matière de lutte contre ces menaces. Les cyberactivités des criminels et des gangs du crime organisé qui sont motivés par un profit financier ou matériel sont exclues de la présente étude.

### CONTEXTE

La plupart des infrastructures essentielles ont trois caractéristiques communes : leur importance ou pouvoir symbolique, le degré de dépendance à l'infrastructure pour le bon fonctionnement de la société, et l'immédiateté de cette dépendance, ainsi que les effets connus et non prévus des dépendances complexes qui ont des conséquences qui vont au delà de l'échelle locale. Chaque pays possède une définition différente de la criticité, mais toutes ces définitions ont en commun l'existence d'un élément informatisé sur lequel dépendent les systèmes physiques qui, s'il est perturbé, pourrait causer des dommages étendus sur le plan physique[1].

Le lien entre « cyber » et infrastructures essentielles était déjà reconnu au changement du millénaire, puisque le Canada (et d'autres administrations) faisait face au soi-disant bogue de l'an 2000, qui a entraîné la création du Bureau de la protection des infrastructures essentielles et de la protection civile (BPIEPC). Le terme « cyberattaques » est communément utilisé pour décrire une variété de cyberincidents qui sont lancés dans différents buts par divers acteurs (individus, groupes criminels organisés, groupes plus ou moins affiliés et États)[2].

Les menaces pesant contre les infrastructures essentielles ont d'abord été jugées comme une principale préoccupation en matière de sécurité nationale dans la politique canadienne de sécurité nationale « Protéger une société ouverte » (2004)[3]. Dans la Stratégie nationale sur les infrastructures essentielles[4], lancée en mai 2010, on a ensuite cerné dix secteurs des infrastructures essentielles et on a demandé à chacun des ministères et organismes concernés d'en assurer la protection. La responsabilité générale de promouvoir la résilience des infrastructures essentielles relève de Sécurité publique Canada. La responsabilité des secteurs des infrastructures essentielles est répartie comme suit :

- Énergie et services publics : Ressources naturelles Canada
- Technologies de l'information et de la communication : Industrie Canada
- Finances : Finances Canada
- Alimentation : Agriculture et Agroalimentaire Canada
- Santé : Agence de la santé publique du Canada
- Secteur manufacturier : Industrie Canada, Défense nationale
- Sécurité : Sécurité publique Canada
- Transport : Transports Canada
- Eau : Environnement Canada

La Stratégie nationale sur les infrastructures essentielles prévoit une approche tous risques et reconnaît non seulement qu'il existe des interdépendances au sein des secteurs et entre ceux-ci, mais aussi qu'elles sont davantage intensifiées par la dépendance accrue envers les technologies de l'information et de la communication (TIC). La Stratégie comprend un plan d'action qui met l'accent sur l'établissement de partenariats entre les divers ordres de gouvernement, le secteur privé et d'autres intervenants, tout en reconnaissant que la responsabilité de la protection des biens est d'abord celle des propriétaires et exploitants des infrastructures essentielles[5].

Dans le cadre de l'approche de partenariat, on a établi des réseaux sectoriels qui relèvent de leur ministère responsable respectif. La plupart de ces réseaux sectoriels sont composés de propriétaires et d'exploitants du secteur, le plus souvent par l'entremise de leurs associations industrielles nationales, ainsi que des ministères et organismes fédéraux, provinciaux et territoriaux concernés. Leur rôle est de servir de forums nationaux permanents propres à leur secteur pour se pencher sur des questions d'intérêt commun concernant la protection des infrastructures essentielles et pour faciliter l'échange d'information et l'obtention

de rétroaction de la part de l'industrie. Comme ces réseaux sectoriels se trouvent à différentes étapes sur les plans de la maturité et de l'expérience, la circulation d'information qui en découle, les évaluations des vulnérabilités entre les secteurs et leurs interdépendances manquent d'uniformité et de cohérence.

En outre, le Forum national intersectoriel a été mis en place pour permettre aux représentants des réseaux sectoriels et aux gouvernements fédéral, provinciaux et territoriaux d'échanger de l'information et de se pencher sur les dépendances entre les secteurs. Les membres du Forum se réunissent tous les ans depuis 2010.

La Stratégie de cybersécurité du Canada[6], adoptée en octobre 2010, prévoit un plan d'action pour participer, avec les provinces, les territoires et le secteur privé, à la mise en œuvre d'une stratégie de cybersécurité visant à protéger les systèmes numériques du pays. Elle préconise une évaluation approfondie des menaces, des vulnérabilités et des risques associés aux infrastructures essentielles du Canada qui découlent de cyberattaques. La Stratégie vise à se fonder sur un cadre de partenariat mis en place au titre de la Stratégie nationale sur les infrastructures essentielles, plus particulièrement en ce qui concerne les intervenants du secteur privé[7].

La Gendarmerie royale du Canada (GRC) a formé l'Équipe des renseignements relatifs aux infrastructures essentielles pour examiner les menaces physiques et cybernétiques pesant contre les infrastructures essentielles, dont l'un des outils est le Système de signalement des incidents suspects. Cet outil vise à recueillir de l'information de l'industrie privée et des organismes d'application de la loi locaux à propos d'incidents suspects.

Depuis l'automne 2011, le Centre canadien de réponse aux incidents cybernétiques (CCRIC) de Sécurité publique Canada (SP) a été déplacé au sein du Secteur de la gestion des mesures d'urgence et de la sécurité nationale en tant qu'entité désignée pour la coordination des interventions du gouvernement fédéral en cas d'incidents d'intérêt commun touchant la cybersécurité et la protection des infrastructures essentielles. Le CCRIC a entre autres la responsabilité de surveiller les cybermenaces, de coordonner la gestion des incidents et de faciliter l'échange d'information dans le but de protéger les infrastructures essentielles.

En février 2012, Sécurité publique Canada a lancé la Stratégie antiterroriste du Canada, intitulée *Renforcer la résilience face au terrorisme*, qui préconise une approche intégrée à plusieurs volets en matière de protection des Canadiens et des intérêts canadiens contre les attaques terroristes. Elle vise à pousser les organismes d'application de la loi à miser leurs efforts sur des objectifs stratégiques clairs[8]. La Stratégie reconnaît explicitement que les groupes terroristes ont exprimé leur intention de renforcer leurs capacités en vue de lancer des attaques informatiques contre les infrastructures essentielles[9]. Grâce à son élément « priver », la nouvelle Stratégie permettra d'organiser des programmes et des activités visant à réduire les vulnérabilités potentielles en matière de sécurité dans le domaine cybernétique, ainsi que dans d'autres domaines des infrastructures essentielles du Canada[10].

## DYNAMIQUES STRUCTURELLES DES SECTEURS DES INFRASTRUCTURES ESSENTIELLES AU CANADA

Chacun des quatre secteurs abordés dans la présente étude possède des sous secteurs industriels ou économiques uniques qui ont leurs propres structure, caractéristiques opérationnelles et vulnérabilités. La plupart d'entre eux appartiennent au secteur privé et sont exploités par celui-ci. Les diverses composantes des infrastructures essentielles mènent leurs activités dans un environnement économique concurrentiel à l'échelle internationale, dont les progrès technologiques, surtout les TIC, représentent un élément moteur de plus en plus puissant.

### ÉNERGIE ET SERVICES PUBLICS

Le secteur de l'énergie et des services publics comprend l'extraction et le raffinage de pétrole et de gaz naturel, les oléoducs, la production et la transmission d'électricité, ainsi que la production d'énergie nucléaire. En 2010, la production, le traitement et la livraison de pétrole, de gaz et d'électricité ont contribué à 6,2 % du produit intérieur brut (PIB) du Canada. L'industrie canadienne de l'énergie possède un degré élevé de criticité pour les économies nationale, provinciale et locale, les consommateurs, les industries utilisatrices et le bien être général du public. Au cours des dernières années, le secteur de l'énergie a atteint sa capacité ou l'a presque atteinte, plus précisément en ce qui concerne la production d'électricité et le raffinage du pétrole, et il a

présenté peu de redondance facilement accessible, pour ne pas dire aucune. Une perte soudaine de la capacité à cet égard en raison d'un dommage majeur aux infrastructures énergétiques causerait des pénuries d'approvisionnement immédiates, ce qui entraînerait une montée en flèche des prix.

Le secteur de l'énergie du Canada est étroitement intégré à l'économie des États-Unis à l'échelle du continent en raison des réseaux d'oléoducs, des réseaux électriques et des interactions commerciales étendues entre les propriétaires et exploitants des infrastructures des deux côtés de la frontière. Le Canada est devenu le plus grand fournisseur international de pétrole et de gaz naturel aux États-Unis.

Les dirigeants de l'industrie pétrolière qui ont pris la parole lors du Congrès mondial du pétrole à Doha, au Qatar, en décembre 2011, ont exprimé leur peur que les cyberattaques contre les infrastructures essentielles puissent faire des ravages en détruisant les établissements ou en perturbant gravement la production et la livraison. En raison des interdépendances entre le secteur de l'énergie et la plupart des autres secteurs économiques et sociaux, ainsi que des exigences relatives à la résidence privée, une perturbation majeure de la disponibilité d'énergie aurait des conséquences profondes et lourdes sur les Canadiens et les marchés d'exportation voisins aux États Unis.

Au cours de la dernière décennie, la structure de l'industrie de l'électricité a fait l'objet de changements importants. La séparation des fonctions de production, de transmission et de distribution de services d'électricité entre diverses organisations a accordé une plus grande importance au rôle du secteur privé, au moment où les investissements du gouvernement fédéral dans la recherche et le développement ont servi à appuyer la commercialisation de nouvelles technologies.

Les réseaux électriques du Canada et des États-Unis sont étroitement interconnectés, et il y a des interdépendances de grande envergure entre leur économie et leur société respectives. Les tendances futures semblent vraisemblablement ouvrir la voie à de nouvelles vulnérabilités dans ces réseaux en raison de la mise en œuvre d'appareils électroniques de communication avancées, y compris les compteurs automatisés et les synchrophaseurs. Ces avancés technologiques risquent de créer de nouveaux vecteurs permettant aux cyberattaquants d'avoir accès aux systèmes informatisés ou à d'autre matériel de communication, causant ainsi des perturbations, voire des pannes d'électricité.

La responsabilité générale d'assurer la fiabilité du réseau électrique incombe au North American Electric Reliability Council (NERC), un organisme indépendant qui vise à promouvoir la fiabilité et la sécurité du réseau de production transport d'électricité aux États-Unis, au Canada et dans certaines parties du Mexique. Le NERC établit les normes de l'industrie et surveille la conformité à celles-ci, en plus de fournir une expertise technique au regard des analyses et des recherches de preuves judiciaires relatives aux pannes d'électricité. Il oblige les entreprises d'exploitation à désigner les biens cybernétiques essentiels et à adopter des mesures de sécurité physiques et cybernétiques adéquates.

## TRANSPORT

L'infrastructure du transport du Canada englobe les transports aérien, maritime et ferroviaire, les ports, le transport urbain, le réseau routier, les ponts et les tunnels. Le secteur du transport joue un rôle très important relativement à l'économie et à la société canadiennes.

Parmi les nouvelles tendances en matière de transport urbain figurent les plans conçus par l'entreprise Bombardier inc. du Canada en vue de mettre en œuvre un système de transport public électronique complètement intégré et sans contact appelé « Primove », qui utilisera la technologie sans fil pour recharger la batterie en continu, ainsi que pour les horaires, les billets, l'entretien et d'autres fonctions. Cette technologie permettrait de gérer un grand nombre de véhicules de transport public électroniques partageant la même infrastructure de base.

## FINANCES

L'infrastructure financière comprend les opérations bancaires, les assurances, les marchés financiers, les services d'acceptation des cartes de crédit et de débit, le courtage et les services financiers. Ensemble, les finances, les assurances et l'immobilier, ainsi que la location et la gestion des entreprises, ont contribué à environ 20 % du PIB du Canada en 2011, ce qui représente de loin le plus grand segment de l'économie canadienne.

Les banques et les institutions financières du Canada dépendent fortement des systèmes de TI et de télécommunications relativement à la gestion des paiements quotidiens et des activités de compensation et de règlement.

Un approvisionnement en électricité sécuritaire et résilient dans ces secteurs est également essentiel. Le ministère des Finances estime que les banques canadiennes ont plus de 8 000 succursales et presque 18 000 guichets automatiques bancaires (GAB) dans tout le pays. En effet, le Canada est le pays où le nombre de guichets automatiques par personne est le plus élevé au monde et bénéficie des taux de pénétration les plus élevés pour ce qui est des canaux électroniques, comme les cartes de débit, les services bancaires par Internet et les services bancaires par téléphone.

## TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION (TIC)

Le secteur des TIC englobe la téléphonie, la radiodiffusion et la télédiffusion, la connectivité Internet, les contrôles de l'accès au périmètre ainsi que la surveillance et le contrôle des satellites. Dans un environnement concurrentiel à l'échelle mondiale, les propriétaires et exploitants canadiens d'infrastructures essentielles, tout comme leurs homologues partout ailleurs, ont de plus en plus tendance à mettre en œuvre des cybertechnologies sophistiquées afin de favoriser les économies et l'efficacité opérationnelle.

Parmi ces nouvelles technologies, mentionnons les systèmes de contrôle informatisés qui sont utilisés par bon nombre d'industries et d'infrastructures essentielles canadiennes pour surveiller et contrôler les processus délicats et les fonctions physiques. De manière générale, les systèmes de commande répartis sont utilisés dans une seule centrale ou usine de traitement, ou dans une petite région géographique, alors que les systèmes d'acquisition et de contrôle des données (SCADA) sont utilisés pour mener de vastes opérations de distribution géographiquement dispersées. De tels systèmes de contrôle exécutent des fonctions essentielles au sein des secteurs des infrastructures essentielles, notamment la production, le transport et la distribution d'électricité; le raffinage du pétrole et du gaz et les oléoducs; le traitement et la distribution d'eau, ainsi que les systèmes ferroviaires et de transport en commun. Toutefois, l'adoption de technologies normalisées qui ont des vulnérabilités connues, l'augmentation de la connectivité de ces systèmes de contrôle avec d'autres, l'insécurité des cyberconnexions à distance et la grande disponibilité de l'information technique concernant les systèmes de contrôle ont contribué à accroître les risques de cyberattaques. La vulnérabilité des communications par Internet pose des risques importants aux infrastructures essentielles et aux activités qu'elles mènent.

Les TIC sont utilisées dans le secteur du transport pour les réservations des voyageurs aériens, le contrôle relatif à l'embarquement et la gestion de la cargaison aérienne. Elles font également partie des programmes Expéditions rapides et sécuritaires et Pre-arrival Processing System (système PAPS), qui facilitent les autorisations préalables à la frontière pour les camions. Les systèmes de TIC connectés à Internet sont utilisés dans le secteur des finances pour les comptes clients (GAB), les appareils de paiement par cartes de débit ou de crédit et les virements de fonds. (Voir l'annexe A pour obtenir de plus amples renseignements sur les dynamiques structurelles du secteur des TIC.)

## INFRASTRUCTURES ET INTERDÉPENDANCES

Les quatre secteurs des infrastructures essentielles dont il est question dans le présent document sont « essentiels » dans la mesure où ils produisent, directement ou indirectement, des extrants essentiels au bien-être économique et social des Canadiens. L'énergie et les services publics de même que les TIC constituent aussi des extrants essentiels à d'autres secteurs des infrastructures essentielles. Tout dommage ou toute perturbation de leurs activités ou des produits ou services qu'ils fournissent aura de graves répercussions.

Les infrastructures nationales essentielles sont confrontées à une grande panoplie de menaces physiques, y compris les phénomènes météorologiques extrêmes, le vandalisme, les pannes électriques, le vol de matériel. Cette vulnérabilité augmente selon la dépendance ou la connexion à une autre infrastructure, qu'il s'agisse d'un lien physique, géographique ou cybernétique.

On entend par *dépendance* un lien où un produit ou un service est lié à un autre produit ou service ou est influencé par ce dernier. Par exemple, *au sein* du secteur de l'énergie, l'approvisionnement en pétrole dépend énormément de l'approvisionnement en électricité, car les raffineries, les oléoducs et les pompes à essence des stations-service ont besoin d'électricité pour fonctionner. Il y peut aussi y avoir une dépendance *entre* les secteurs; la disponibilité des moyens de transport routier, ferroviaire et côtier est essentielle pour acheminer les produits énergétiques aux consommateurs. Il y a des *interdépendances* lorsque les producteurs et les fournisseurs de produits et de services, tant au sein qu'entre les secteurs des infrastructures essentielles, deviennent dépendants l'un de l'autre, même à des degrés divers et inégaux.

La principale caractéristique d'une société moderne, interconnectée et axée sur le savoir et de son économie est la dépendance aux TIC. L'infrastructure numérique qui relie les dix secteurs des infrastructures nationales essentielles est à la fois une ressource nationale stratégique à part entière ainsi qu'une priorité en matière de sécurité, car l'appareil gouvernemental, les infrastructures nationales essentielles et la prestation de services essentiels comme l'eau, le pétrole, l'électricité, les communications et les services bancaires dépendent tous grandement des TIC. De telles interdépendances peuvent avoir de graves répercussions commerciales et sociales s'il y a des perturbations dans la disponibilité de produits et de services comme l'énergie, les transports ou les réseaux de communication.

Les conséquences se répercutent non seulement sur l'ensemble des secteurs, mais aussi sur l'ensemble des administrations (privées, publiques, provinciales, territoriales et fédérale). Pour protéger efficacement ces liens cybernétiques essentiels, il faudra probablement de nouvelles initiatives défensives et proactives couvrant les domaines de la technologie, de l'éducation, des politiques et de la loi. Bien que les technologies de l'information et des communications offrent aux entreprises des possibilités, celles-ci ont un coût, à savoir une vulnérabilité accrue aux diverses menaces inhérentes à la mondialisation.

La protection des liens directs et indirects entre les infrastructures qui soutiennent les installations essentielles ainsi que la prévention de leurs défaillances nécessitent une compréhension pointue des fonctions organisationnelles et des répercussions opérationnelles afin de pouvoir déterminer comment et où les structures internes établissent des liens avec les infrastructures externes. Une connectivité accrue augmente la probabilité d'avoir des effets imprévus au-delà de l'échelon local; c'est ce qu'on appelle parfois *l'effet papillon*. En raison de la complexité des liens, l'obtention d'une connaissance de la situation suffisamment exhaustive représente un défi de taille. Par contre, une fois que de nouvelles technologies, de nouveaux processus et de nouvelles pratiques ont été trouvés, ils peuvent contribuer à restreindre, à dissiper et à atténuer les perturbations.

Des ensembles de réseaux et de systèmes étroitement connectés sont reliés les uns aux autres à de nombreux points à l'aide d'une vaste panoplie de mécanismes physiques et électroniques. En raison des technologies des communications de l'information, les interdépendances complexes des infrastructures essentielles ont rendu les secteurs clés de plus en plus vulnérables aux attaques perpétrées contre ces réseaux.

À titre d'exemple, les systèmes de transmission de données et les méthodes automatisées de commande et de contrôle (SCADA) sont très répandus sur l'ensemble des infrastructures essentielles du Canada. Ces systèmes SCADA connectés à Internet permettent une surveillance et un contrôle centralisés des processus de production et de prestation, que ce soit dans des installations précises ou dans des infrastructures complexes interdépendantes qui sont réparties sur de vastes territoires. Les espions, les terroristes et les cybermilitants malveillants cherchent à pénétrer ces réseaux pour obtenir de l'information, pour perturber les services ou pour lancer d'autres attaques. Les secteurs de l'énergie, du transport et des finances sont particulièrement vulnérables à ce type de perturbations, lesquelles peuvent avoir des répercussions dramatiques sur d'autres secteurs, comme celui de la santé.

Les institutions publiques et les entreprises commerciales utilisent de plus en plus des technologies à large bande et sans fil, fixes ou mobiles, pour leurs services de télécommunication; les deux dépendent d'un approvisionnement constant en électricité. Bien que les stations de base mobiles soient dotées de piles de secours, celles-ci ne durent habituellement que peu de temps, ce qui rend ces stations vulnérables aux pannes de l'alimentation principale. De plus, puisque les services sans fil sont connectés aux infrastructures de télécommunication principales, tout problème important qui touche les téléphones terrestres peut aussi mettre hors service les points d'accès sans fil. Même lorsque cela n'est pas le cas, une hausse soudaine de l'utilisation peut surcharger les services de téléphonie cellulaire comme ce fût le cas immédiatement après les attentats à la bombe survenus le 7 juillet 2005 à Londres.

Les interdépendances entre toutes les diverses infrastructures ne peuvent probablement pas toutes être connues, mais une connectivité accrue signifie que la défaillance d'une composante essentielle pourrait avoir des effets de grande portée. Les divers types de défaillances peuvent être divisés comme suit :

a) *Défaillance d'origine commune* – Diverses installations (stockage de carburant, aéroports et centrales électriques) qui sont situées à proximité risquent d'être touchées par un même incident d'inondation;

b) *Défaillances en cascade* – La perturbation d'un système de contrôle dans une infrastructure (p. ex. approvisionnement en électricité ou en eau) menant à la perturbation d'une autre infrastructure (comme le transport ferroviaire, si les

signaux ne fonctionnent pas), puis à celle d'une troisième infrastructure (p. ex. une chaîne d'approvisionnement alimentaire), et ainsi de suite, et ce, même s'il n'y a aucune dépendance *directe*. Une cyberattaque pourrait directement influer sur de telles défaillances en cascade.

c) *Défaillance aggravante* – La perturbation d'une infrastructure (un réseau de communication) nuit aux mesures visant à réparer d'autres infrastructures qui ont été endommagées par d'autres entités (p. ex. les services d'urgence, les commerces).

Les récentes perturbations qu'a connues l'aviation civile, une infrastructure de base dans les sociétés développées, illustrent bien le caractère essentiel des liens physiques et géographiques avec l'industrie; par contre, toute perturbation dans le fonctionnement des systèmes informatiques servant au contrôle de la circulation aérienne pourrait nuire à l'ensemble de la circulation aérienne. La grande utilisation des systèmes SCADA accroît la vulnérabilité aux cyberattaques dans d'autres secteurs des infrastructures essentielles, qui à leur tour feront l'objet des effets en cascades et aggravants de ces perturbations.

Les processus permettant de cerner les interdépendances et les vulnérabilités physiques et informatiques connexes nécessitent que les intervenants travaillent ensemble afin d'appliquer les bonnes stratégies pour réduire les risques lorsque cela est possible, de combler les lacunes en matière de préparation et d'atteindre la résilience notamment en assurant un certain niveau de substituabilité et de redondances prévues. Les experts ont élaboré et utilisent des outils pour tenir compte de la complexité des infrastructures nationales interdépendantes, y compris les systèmes fondés sur les processus, les modèles dynamiques, les modèles mathématiques d'optimisation des réseaux, les modèles fondés sur la physique des infrastructures en place et les systèmes de simulations haute-fidélité en mode agent.

De nombreux propriétaires et exploitants du secteur privé ne sont pas suffisamment conscients des interdépendances actuelles qui pourraient avoir des répercussions tant sur les fournisseurs de services dont ils dépendent que sur leur propre capacité à continuer leurs activités et à offrir des services à leurs clients. Leur vulnérabilité aux effets en cascade d'une défaillance des TIC dans un autre élément de leur chaîne opérationnelle rend la tâche difficile aux intervenants pour ce qui est d'exécuter la tâche fondamentale qu'est la gestion du risque : établir la priorité des risques informatiques en vue de déterminer ceux qui

peuvent être tolérés, ceux qui peuvent être évités ou déplacés à l'avance et ceux qui nécessitent absolument des mesures d'atténuation. Les propriétaires et les exploitants qui ne sont pas suffisamment conscients de ces questions ne peuvent pas eux-mêmes réduire les risques, car les interdépendances nécessitent une approche collaborative entre les secteurs privé et public.

# CHAPITRE 2
# CONTEXTE DE LA MENACE CYBERNÉTIQUE

Il convient de distinguer les mesures qui sont prises pour des fins de collecte de renseignements des mesures qui sont prises pour des raisons politiques ou idéologiques, lesquelles sont délibérées et visent à modifier, à perturber, à tromper, à dégrader, à détruire les systèmes et les services informatiques ainsi qu'à en empêcher l'utilisation, c'est-à-dire à les rendre non disponibles ou non fiables. Ces menaces découlent du terrorisme international (qui peut être encouragé et facilité par l'ingérence étrangère ou des entités gouvernementales), des actes d'espionnage et de sabotage parrainés par l'État, ainsi que de l'hacktivisme malveillant et peuvent supposer la participation d'une personne faisant partie de l'organisation, qui est à l'origine de l'attaque ou qui y prend part. Les menaces internes sont celles qui sont posées par du personnel qui a été suborné ou « placé » dans l'organisation pour des fins hostiles. Il est rare que l'information de sources ouvertes soit disponible sur les menaces internes manifestes puisque les organisations ont tendance à être réticentes lorsqu'il s'agit de questions de ce genre, et ce, pour des motifs liés à la réputation.

L'affaire WikiLeaks, qui s'est passée en 2010 et qui aurait découlé d'une fuite interne, a engendré le dévoilement de milliers de câbles diplomatiques américains et a soulevé des questions au sujet de la valeur et de la vulnérabilité des ressources d'information informatisées de nature politique et délicate. En raison de ce genre d'attaques et d'autres genres d'attaques contre des systèmes informatiques, des documents gouvernementaux ont été obtenus, et des renseignements confidentiels de particuliers et d'entreprises ont été dévoilés et compromis. C'est lorsque la cible n'est pas au courant qu'il y a eu atteinte aux données et que le fonctionnement normal du système n'est pas perturbé que ces activités sont les plus efficaces.

Les TIC ont la caractéristique suivante : grâce à leur grande accessibilité, combinée à des compétences quasi universelles en matière de technologie informatique, les pirates informatiques potentiels peuvent provenir d'un large spectre. Ces pirates informatiques peuvent comprendre des organismes officiels, des groupes peu structurés et même des personnes. Les motivations peuvent aller des protestations légitimes à l'espionnage, en passant par la promotion de l'extrémisme. À l'extrémité très organisée du spectre, l'Armée de libération populaire de Chine aurait déployé une unité spécialisée de renseignements d'origine électromagnétique aux fins du cyberespionnage; à l'extrémité la moins

structurée du spectre se trouvent les groupes anarchistes, les activistes contre la mondialisation et les hacktivistes malveillants comme le groupe Anonymous, qui n'utilisent aucune structure hiérarchique et qui fonctionnent de façon itérative, consensuelle et communautarienne. Al-Qaïda et les groupes qui y sont affiliés, qui sont organisés en fonction d'un leadership stratégique, mais qui ont toutefois un réseau opérationnel réparti aux quatre coins du monde, et qui comptent des membres hautement qualifiés dans le domaine du génie informatique, se trouvent entre ces deux extrêmes.

L'analyse qui suit cerne les vulnérabilités et porte sur les intentions déclarées, les stratégies, les objectifs et les capacités démontrées des entités réputées d'avoir menacé les infrastructures essentielles du Canada, y compris les systèmes d'information du gouvernement. Les menaces comprennent les suivantes :

- terrorisme international, plus particulièrement al-Qaïda et les groupes qui y sont affiliés;
- actes de terrorisme, d'espionnage et de sabotage parrainés par des États;
- hacktivisme malveillant;
- menaces internes.

Bien que les nombreux exemples mentionnés ci-après soient classés dans l'une de ces catégories, il doit être évident que la cyberdimension brouille les lignes qui les démarquent. En effet, au tout début d'une attaque, il peut être impossible de préciser si le pirate informatique est parrainé par un État, s'il est autonome ou s'il est membre d'un groupe malveillant ou criminel. Les coïncidences et la complexité de la motivation et des moyens font de l'attribution – soit la reconstitution de l'événement jusqu'à l'entité d'origine – un processus long et complexe, qui peut ne jamais être mené à terme de façon satisfaisante.

## TERRORISME INTERNATIONAL

Dans la nouvelle Stratégie antiterroriste du Canada, *Renforcer la résilience face au terrorisme*, on désigne « la violence inspirée par le mouvement extrémiste islamiste sunnite » comme « la principale menace pour la sécurité nationale du Canada » . Selon la Stratégie :

> « Al-Qaïda, dirigée par Ayman al-Zawahiri depuis la mort d'Oussama Ben Laden en mai 2011, demeure aux premières lignes de l'extrémisme islamiste sunnite. Ce groupe continue de servir de source idéologique et d'inspiration pour les terroristes potentiels partout dans le monde. Même si les efforts d'antiterrorisme déployés partout dans le monde ont permis de réduire les capacités d'al-Qaïda au cours des dernières années, d'autres groupes islamistes sunnites associés à al-Qaïda, que ce soit parce qu'ils lui ont officiellement prêté allégeance ou qu'ils le prennent pour modèle, ont gagné en importance et représentent une grave menace pour le Canada et la communauté internationale »[12].

Dans la Stratégie, on précise que c'est depuis longtemps que les groupes terroristes ciblent la protection des infrastructures essentielles, en particulier de l'aviation civile[13].

Al-Qaïda et les groupes qui y sont associés ont fait preuve d'une agilité remarquable en se transformant en un réseau mondial élusif et éclectique de groupes, de cellules et d'auxiliaires nationaux capables de perpétrer des attaques mortelles contre les ennemis perçus de l'islam. De par leur discours religieux, leur doctrine tactique et leurs opérations, al-Qaïda et les groupes associés menacent explicitement et directement les infrastructures économiques des pays ciblés, qui comprennent le Canada. Leur soi-disant djihad économique[14] vise à désorienter et à étouffer (leur) économie et à menacer (leur) avenir économique et politique[15]. Les cibles prioritaires comprennent les propriétés appartenant au gouvernement, les banques, les sociétés mondiales, ainsi que « les richesses appartenant aux non croyants qui ont une animosité connue à l'égard des musulmans »[16]. L'objectif stratégique, pour citer Oussama Ben Laden, était de saigner l'Amérique jusqu'à la faillite[17].

Les infrastructures énergétiques, en particulier les installations pétrolières, les pipelines et les pétroliers, ressortent comme étant une cible primaire pour le djihad économique. Les attaques relatives aux infrastructures énergétiques visent à endommager et à affaiblir les économies des ennemis perçus de l'islam, d'abord et avant tout celle des États Unis, de façon à réduire leur capacité industrielle, financière et militaire à faire face aux attaques des djihadistes. Le Canada, qui est l'exportateur de pétrole et de gaz naturel le plus important aux États Unis, ainsi que ses infrastructures énergétiques, ont été menacés de façon explicite. Par ailleurs, des intérêts d'entreprises pétrolières canadiennes au Yémen ont également été la cible d'attentats.

De façon semblable, l'aviation civile est une cible importante pour le terrorisme d'al-Qaïda et pour les terroristes internationaux en général, comme le mentionne le document sur la nouvelle Stratégie antiterroriste du Canada[18]. Les vols de passagers, les vols de transport de marchandises et les installations aéroportuaires ont tous été la cible d'attentats terroristes dans le cadre du djihad économique proclamé par al-Qaïda contre l'Ouest[19]. Un complot de 2006, surnommé « Operation Overt » par la police britannique, a entraîné l'arrestation, puis la condamnation et une peine d'emprisonnement à vie d'une cellule inspirée d'al-Qaïda qui a planifié des attentats suicide à la bombe sur des vols transatlantiques à destination de l'Amérique du Nord. À la suite d'un complot déjoué en 2010, qui visait à faire exploser un avion de fret en vol au-dessus de l'Amérique du Nord, dans le cadre de l'opération surnommée « Hémorragie », le planificateur opérationnel d'al-Qaïda a affirmé que leur « objectif n'était pas de causer un maximum de décès, mais de causer le plus de pertes possible pour l'économie américaine »[20].

Dans une déclaration qui a suivi vantant le djihad économique, l'idéologue d'al-Qaïda Yahya Ibrahim a donné un avertissement public : [traduction] « [N]ous continuerons de mener des opérations de ce genre… Nous exposons d'avance notre plan à nos ennemis parce que comme nous l'avons affirmé précédemment, notre objectif n'est pas de tuer le plus de personnes possible, mais de causer une hémorragie dans l'industrie de l'aviation, industrie essentielle pour le commerce et le transport entre les États Unis et l'Europe »[21].

Aussi, dans le secteur des transports, des services ferroviaires voyageurs et des réseaux de transport en commun dans plusieurs pays, y compris en Allemagne, en France, en Espagne, au Royaume-Uni et aux États-Unis, ont été ciblés par des groupes djihadistes internationaux ou intérieurs affiliés avec l'organisation d'al-Qaïda ou inspirés de celle-ci. Selon la Transportation Security Administration des États-Unis, des pirates informatiques non identifiés, qui seraient de l'étranger, ont lancé des cyberattaques contre une compagnie ferroviaire américaine, ce qui a causé la perturbation de la signalisation et du trafic ferroviaire dans le Nord-Ouest des États-Unis pendant deux jours, en décembre 2011.

///

*Conformément au concept du djihad économique, Ayman al-Zawahiri a publié une déclaration vidéo en février 2011, dans laquelle il demande aux djihadistes d'innover et de trouver de nouvelles façons et de nouvelles méthodes pour attaquer les infrastructures de grande valeur : [traduction] « Si nous ne sommes pas en mesure de produire des armes équivalant à celles du croisé occidental, nous pouvons saboter ses systèmes économiques et industriels complexes et le déposséder de ses pouvoirs… Ainsi, les mujahideen [guerriers islamiques] doivent inventer de nouvelles méthodes, des méthodes qui ne sont jamais venues à l'esprit de l'Occident »*[22].

La première cyberattaque terroriste à grande échelle qui a relativement bien réussi est une attaque contre les systèmes informatiques gouvernementaux qui a été attribuée au groupe Tariq bin Ziyad Brigades pour le djihad électronique et qui s'est produite en 2010. Bien qu'aucun élément probant ne soit encore disponible au sujet du cyberterrorisme de la part d'al-Qaïda ou des groupes qui y sont affiliés, la stratégie antiterroriste mise à jour du Royaume-Uni [« CONTEST 2 »] présentée en juillet 2011, donnait un avertissement selon lequel à la suite du décès d'Oussama Ben Laden, l'organisation d'al-Qaïda avait recommandé explicitement un cyberdjihad ainsi que d'autres opérations terroristes[23].

Formulant des commentaires sur les capacités en matière de TI des groupes terroristes islamistes, les représentants du gouvernement des États-Unis ont admis qu'ils avaient sous estimé le temps qu'al-Qaïda avait passé à tenter de trouver les faiblesses des États-Unis. Les autorités américaines auraient découvert que des employés utilisaient des commutateurs de télécommunication dans plusieurs pays, y compris en Arabie-saoudite et au Pakistan, afin d'explorer les systèmes numériques qui contrôlent les centrales nucléaires, les services téléphoniques d'urgence et les réseaux de stockage et de distribution d'eau. Un ordinateur saisi dans une installation secrète d'al-Qaïda à Kaboul contenait un programme de génie utilisé pour localiser les faiblesses structurelles dans les immeubles, les ponts et les barrages.

Certains érudits islamiques ont récemment souligné qu'ils étaient en faveur du nouveau phénomène qu'est le djihad électronique, affirmant que toute tentative pour exaspérer l'ennemi et appuyer la religion est légitime[24]. Ils jugent que les jeunes musulmans qui participent à ce phénomène dirigent en réalité un djihad.

Al-Qaïda et ses groupes affiliés ainsi que les groupes auxiliaires nationaux démontrent depuis longtemps leurs capacités en matière de TIC pour leurs propres fins. Dans un rapport spécial préparé pour l'Institute of Peace des États Unis, le professeur Weimann a cerné huit méthodes que les militants djihadistes contemporains ont employées pour exploiter les capacités d'Internet, notamment pour la guerre psychologique, la propagande et la publicité, le forage de données, les collectes de fonds, le recrutement et la mobilisation, le réseautage de groupe, l'échange d'information ainsi que la planification et la coordination d'attaques réelles.[25] Il importe de mentionner que le recrutement pour le groupe al-Qaïda semble avoir permis d'attirer dans ses rangs un très important contingent de diplômés universitaires en informatique et en technologies de l'information. Selon une étude de l'University of Oxford réalisée par des radicaux islamiques, les ingénieurs informaticiens sont surreprésentés parmi les membres de groupes djihadistes militants aux quatre coins du monde[26].

Il semble évident qu'al-Qaïda et ses groupes affiliés ont accès aux compétences et aux capacités qui sont nécessaires pour lancer une cyberattaque en faveur du djihad économique déclaré, ciblant les infrastructures essentielles du « croisé occidental », y compris celles du Canada. La probabilité que les terroristes lancent des cyberattaques contre leurs ennemis est assez élevée pour faire monter les coûts liés à la sécurité, surtout dans le cas d'al-Qaïda, puisque l'organisation a déclaré un djihad économique et électronique afin d'affaiblir l'économie des États-Unis et celle de ses alliés. Ainsi, les infrastructures essentielles pourraient être ciblées, non seulement comme objectif en soi, mais aussi comme volet d'un objectif stratégique élargi. Il ne fait aucun doute que les organisations terroristes sont une menace pour les réseaux informatiques, mais cette menace est accrue à un point tel qu'elles réussissent à obtenir l'aide de l'État.

## ACTES DE TERRORISME, D'ESPIONNAGE ET DE SABOTAGE PARRAINÉS PAR DES ÉTATS

*Actes de terrorisme parrainés par des États*

Bien que l'Iran et, dans une moindre mesure, la Syrie soient les deux États qui parrainent le plus activement des actes de terrorisme, bien d'autres États

sont incapables d'empêcher les terroristes d'exploiter leur territoire ou leurs ressources. Au Liban, le Hezbollah tient des camps d'entraînement, fait la contrebande d'armes à feu et le trafic de drogues, et entrepose des milliers de roquettes en vue d'attaques contre Israël.

En janvier 2012, le groupe palestinien Hamas a lancé un appel en vue de multiplier les cyberattaques contre Israël. Le porte-parole du groupe, Sami Abu Zuhri, a écrit ce qui suit, dans une déclaration envoyée par courriel aux journalistes se trouvant dans la bande de Gaza : « L'infiltration des sites Web israéliens ouvre de nouvelles possibilités de résistance et marque le début de la guerre électronique contre l'occupation israélienne. »

Le premier ministre d'Israël, Benjamin Netanyahu, a établi le National Cyber Directorate en août 2011 pour empêcher l'infiltration des systèmes informatiques du gouvernement et des entreprises du pays. Toutefois, au début de 2012, des pirates, s'appelant le « groupe xp, le plus important groupe de pirates wahhabite en Arabie saoudite », ont obtenu et affiché des informations sur des milliers d'Israéliens détenteurs de cartes de crédit (janvier 2012) afin de causer un préjudice personnel et financier à « l'ennemi ».

Les groupes extrémistes et terroristes sont souvent composés d'individus possédant des compétences pointues en ingénierie et en informatique. Ils ont donc les moyens de lancer leurs propres cyberattaques. Ils peuvent toutefois accepter d'agir comme intermédiaires pour l'État lorsque les objectifs stratégiques de ce dernier coïncident ou pourraient faire avancer les leurs. Les pires menaces touchant les infrastructures essentielles— les menaces persistantes avancées, qui englobent les vers et virus sophistiqués comme Stuxnet et Duque— proviennent d'États en raison des ressources techniques et financières nécessaires pour les mettre au point. Les responsables de ces attaques peuvent non seulement se servir de ces instruments pour obtenir un accès non autorisé et prendre le contrôle du logiciel qui assure le fonctionnement de l'infrastructure, mais aussi pour introduire un maliciel à des fins d'espionnage ou de sabotage.

La plupart des cyberattaques connues du public sont commises par des groupes de pirates ou des hacktivistes, mais les organismes de sécurité savent depuis longtemps que des États étrangers et des groupes criminels organisés volent quotidiennement des gigabits de données. À la fine pointe et disposant de ressources abondantes, ces derniers ne publicisent pas leurs activités, car, contrairement aux hacktivistes, ils estiment qu'il n'est pas dans leur intérêt de le faire.

*Espionnage et sabotage parrainés par des États*

La priorité est actuellement accordée à la lutte contre le terrorisme, mais d'autres menaces sont une source d'inquiétude croissante. Comme d'autres pays en Occident, en particulier les États-Unis, le Canada dépend beaucoup des réseaux numériques et des communications Internet, ce qui le rend plus vulnérable aux cyberattaques, dont un fort pourcentage serait attribué à des pirates chinois et russes appuyés par leur gouvernement.

À l'instar de l'espionnage *industriel* ou des autres activités illicites visant à accéder à des renseignements exclusifs ou à des technologies dans le but d'obtenir un avantage commercial, l'espionnage *économique ou politique* parrainé par l'État – qui s'entend de l'activité illégale, clandestine ou coercitive que mène un gouvernement étranger ou ses mandataires à des fins stratégiques mondiales – est également à la hausse. La ligne de démarcation entre les deux est souvent très mince, surtout lorsque des entreprises appartenant à l'État sont impliquées.

///

***Les activités d'espionnage contre le Canada ont atteint un niveau aussi, sinon plus, élevé que pendant la guerre froide. Les attaques lancées à partir d'Internet sont la forme d'espionnage qui connaît la croissance la plus rapide. Le Canada est une cible attrayante en raison de son ouverture en tant que société, de ses relations solides sur la scène internationale et de l'avancement de ces industries, notamment dans les domaines des télécommunications, de l'exploitation minière, de l'agriculture, de la biotechnologie et de l'aérospatial.***

En plus de porter atteinte à l'accessibilité et à la fiabilité des services gouvernementaux et des infrastructures essentielles[27], l'espionnage et l'ingérence étrangère peuvent nuire aux intérêts canadiens en cas de vol de renseignements gouvernementaux stratégiques et confidentiels ou encore d'informations ou d'applications politiques et militaires; de perte de biens et de technologies à la fine pointe; de vol de propriété intellectuelle ou d'informations commerciales ou liées aux armes; d'acquisition d'entreprises qui présentent des risques pour les infrastructures essentielles stratégiques du pays; de transfert illégal des technologies à double usage.

En janvier 2011, des pirates, semble-t-il chinois, ont attaqué directement et indirectement des systèmes et réseaux du gouvernement canadien et y ont accédés en envoyant des courriels ciblés et malveillants qui semblaient des messages légitimes.

Il est difficile de détecter ce genre d'activités de collecte de renseignements, car elles ne sont pas conçues pour perturber le fonctionnement normal des systèmes informatiques, ni alerter les utilisateurs que le système a été compromis. L'un des objectifs clés de la stratégie de cybersécurité des États-Unis est d'ailleurs de mettre fin au vol de propriété intellectuelle lié au cyberespionnage[28].

Les outils et les techniques utilisés pour les cyberattaques sont en constante évolution; de plus, ils incorporent de nouvelles technologies informatiques et de nouvelles capacités liées à Internet. Les attaques massives par déni de service distribué (DDoS), comme celle qu'a subie l'Estonie en 2007 et la Géorgie l'année suivante, ont été perpétrées à l'aide de réseaux de zombies envoyant des commandes à d'innombrables ordinateurs infectés afin qu'ils submergent les systèmes ciblés de programmes malveillants. Les sites Web gouvernementaux, le trafic Internet, les opérations bancaires, les médias et les téléphones cellulaires ont tous été touchés. L'ampleur de ces attaques évoquait une participation de la Russie, mais il arrive également que des attaques DDoS soient lancées par des réseaux criminels dont les activités sont à but lucratif et par des hacktivistes qui tentent d'obtenir des renseignements délicats ou de mettre les autorités gouvernementales dans l'embarras.

Une attaque mondiale perpétrée en 2009, que l'on appelle également l'épisode « GhostNet », a été mis au jour par l'Information Warfare Monitor, importante installation cybernétique canadienne. Dans le cadre de cette attaque, qui a infecté plus de 1 000 ordinateurs dans divers pays, les réseaux de plusieurs gouvernements ont été compromis, et on présume que des secrets commerciaux et d'État ont été perdus.

Dans le cadre d'un autre événement cybernétique qui a eu lieu en 2010, pendant une période relativement brève, 15 % du trafic Internet aux États Unis a été mystérieusement redirigé vers la Chine avant de se rendre aux destinataires. Le Canada n'est pas à l'abri de telles activités : en janvier 2011, un certain nombre de systèmes du gouvernement fédéral ont été la cible d'attaques. De grandes sociétés, le Pentagone et des cabinets d'avocats aux États Unis, en Grande-Bretagne et au Canada sont parmi les organisations qui ont subi des

atteintes à leurs données au cours des dernières années, dont beaucoup auraient été liées à des ordinateurs en Chine. Des pirates informatiques se trouvant en Chine auraient ciblé des cabinets d'avocats dans le cadre de leurs efforts visant à contrer l'offre publique d'achat lancée par la société BHP Billiton pour la Potash Corporation of Saskatchewan, favorisant ainsi les intérêts de la Chine en vue de l'acquisition de ressources naturelles. Une série d'attaques répandues qui se sont produites en août 2011 (surnommée « opération Shady RAT » [RAT : Random Access Tool, soit « outil à accès sélectif » en français]) et qui auraient été parrainées par la Chine, ont ciblé 72 organisations aux quatre coins du monde, y compris les Nations Unies, des gouvernements, des sociétés et le gouvernement du Canada.

Bien que l'espionnage commercial contre des multinationales comme Google, Sony et Lockheed Martin puissent avoir des conséquences de nature stratégique, les menaces persistantes avancées, qui ciblent les réseaux gouvernementaux, organisationnels et de contrôle depuis peu, et ce, au moyen de virus de pointe et de vers informatiques, sont une source de préoccupations importantes. Elles semblent viser la navigation et le mappage d'information et de systèmes de contrôle desquels l'intégrité et la disponibilité des infrastructures essentielles nationales, comme les réseaux électriques, les centrales nucléaires ou les réseaux financiers, dépendent. En infectant les systèmes de contrôle, ces menaces peuvent non seulement fournir les moyens de copier et de voler de l'information au sujet de la conception et des technologies d'exploitation, mais elles peuvent aussi être programmées pour endommager ou détruire les infrastructures à une date ultérieure, par exemple en temps de crise ou de guerre.

Les ressources nécessaires à l'élaboration de ces virus et de ces vers proviennent soit de la participation directe de l'État, soit du parrainage par l'État de mandataires, comme des criminels, des terroristes ou des pirates informatiques. Les États ont de plus en plus tendance à utiliser des intervenants qui n'ont pas de liens avec l'État, lesquels agissent comme des intermédiaires, afin de masquer leur implication. La Chine et la Russie possèdent des capacités prodigieuses pour ce qui est de l'environnement cybernétique; c'est aussi le cas pour l'Iran, la Corée du Nord et même le Myanmar , mais de telles attaques sont contestables parce que le processus d'attribution est complexe[29]. Les intervenants qui n'ont pas de lien avec l'État sont souvent très au courant de la valeur des armes informatiques du genre, mais bien qu'ils n'aient pas la capacité organique de lancer eux-mêmes une attaque, ils peuvent être « embauchés ».

Bien que jusqu'à maintenant, aucun dommage et aucune perturbation n'a été causé, les logiciels inactifs laissés dernière peuvent être programmés pour contrôler, perturber ou détruire certains éléments du système ciblé au moment choisi par l'auteur de l'attaque. Il s'agit clairement d'une menace à la sécurité nationale, et une menace qui soulève d'importantes préoccupations en raison des faiblesses en matière de cybersécurité qui ont été cernées par les organismes de réglementation et les associations des propriétaires et des exploitants des infrastructures essentielles.

De telles attaques s'apparentent aux armes cybernétiques stratégiques – un facteur qui pourrait changer la donne et qui est décrit comme comparable à l'arrivée des armes nucléaires. Même s'il existe des différences notables entre les attaques nucléaires et les cyberattaques, les deux types d'attaques peuvent avoir des conséquences catastrophiques. Par ailleurs, les armes numériques coûtent moins cher, sont instantanées, ne donnent presque aucun avertissement et représentent peu de risques. Elles peuvent demeurer inactives dans le réseau d'une victime pendant un certain temps après y avoir été dirigées par l'entremise de deux pays intermédiaires ou plus. Il s'agit d'une possibilité qui donne à l'auteur de l'attaque des avantages évidents par rapport à la victime.

En janvier 2012, le gouvernement des États Unis a expulsé la consule générale du Vénézuela à Miami, en Floride, parce qu'elle aurait conspiré avec l'Iran afin de perpétrer des cyberattaques contre des centrales nucléaires américaines. Le plan aurait été mis en œuvre comme réaction aux craintes de l'Iran que son programme nucléaire soit attaqué. Le gouvernement du Vénézuela a réagi à l'expulsion en nommant l'ancienne consule générale ministre de la Défense. En janvier 2012, les autorités azerbaïdjanaises ont arrêté des agents iraniens soupçonnés d'avoir planifié des attaques contre d'importants personnages étrangers, y compris l'ambassadeur d'Iran et un rabbin local, après que ceux-ci aient piraté des sites Web de l'État afin de proférer des menaces et d'afficher des messages haineux contre Israël.

La cyberdimension a modifié le caractère des actes d'espionnage, qui auparavant avaient des traits distinctifs et étaient accomplis par des professionnels du renseignement. Désormais, bien que les motivations idéologiques, politiques et économiques puissent être similaires, des intervenants n'ayant pas de liens avec l'État sont maintenant utilisés, de plus les technologies et les intermédiaires cybernétiques rendent la détection et l'attribution plus difficiles. L'objectif des actes d'espionnage consistant en l'acquisition d'un avantage stratégique par le

vol de secrets afin de déterminer les capacités de l'adversaire, ainsi que ses forces et ses faiblesses peut maintenant être atteint puisque l'utilisation d'intervenants et de moyens qui sont contestables et beaucoup plus variés et éphémères est possible. La même procédure peut être employée par les criminels opportunistes, les concurrents organisationnels ou les États étrangers. Tenter de déterminer les intentions, les cibles et les intervenants peut donc être un exercice élusif, du moins aux premières étapes.

## HACKTIVISME MALVEILLANT

Le piratage informatique est un phénomène qui prend de l'ampleur. Alors que la plupart des incidents de piratage d'ordinateurs et de réseaux informatiques semblent motivés par la criminalité, les protestations ou simplement les défis techniques, l'hacktivisme malveillant par des activistes (ou hacktivistes) qui ciblent des infrastructures essentielles pourrait présenter une menace indéniable pour la sécurité nationale[30]. Des sociétés pétrolières canadiennes et internationales ont indiqué que les cyberattaques de plus en plus fréquentes et bien ciblées contre leurs systèmes d'exploitation et d'information contrôlés par ordinateur par des pirates informatiques, le plus souvent motivées par des intérêts criminels ou commerciaux, pourraient faire des ravages mondiaux en perturbant l'approvisionnement en pétrole. Les pirates informatiques peuvent travailler seuls ou avec des groupes plus ou moins structurés de façon informelle qui ont la même philosophie libertarienne ou communautarienne.

L'année dernière, un groupe international de pirates informatique connu sous le nom de « Anonymous » est parvenu à désactiver temporairement des sites de paiement en ligne par carte de crédit et par PayPal pour avoir refusé de transférer des dons à l'organisation WikiLeaks. Plus tard dans l'année, le même groupe d'hacktivistes a brièvement désactivé le site Web de la Bourse de New York en appui aux protestations « Occupons Wall Street ». Puis, à la fin de décembre 2011, Anonymous a annoncé officiellement qu'il interromprait complètement Internet si les États-Unis osaient adopter le projet de loi *Stop Online Piracy Act*. Récemment, Anonymous a fait connaître son intention de cibler les systèmes de contrôle de processus de sociétés pétrolières et gazières dans le cadre de son programme « d'énergie verte », qui appuie spécialement la campagne environnementale contre les sables bitumineux en Alberta et le projet de pipeline *Keystone XL*.

Des éléments faisant partie de certains groupes d'intérêt unique du Canada ont une propension à cibler les infrastructures essentielles par des actions directes violentes dans le cadre de leur programme de protestation. Parmi les éléments les plus radicaux se trouvent ceux qui affirment défendre des causes, anarchistes, environnementales et contre la mondialisation. Étant donné que la plupart de leurs campagnes de protestations visent à attirer l'attention du public, et donc à obtenir de la visibilité, ces groupes semblent moins disposés à avoir recours à des techniques furtives telles que les cyberattaques dans le contexte actuel.

En novembre 2011, un sondage mondial sur la protection des infrastructures essentielles préparé par Symantec Corporation a permis d'en savoir plus sur des attaques menées contre 48 entreprises classées dans le « Fortune 100 » du secteur de la production industrielle de produits chimiques. On a trouvé la trace d'un serveur privé virtuel aux États-Unis à partir duquel les « Nitro Attacks », comme on les a nommées, ont été perpétrées, mais les chercheurs ont finalement découvert que le système appartenait à un homme dans la vingtaine habitant dans la province de Hebei, en Chine.

Le National Cybersecurity and Communications Integration Center des États-Unis estime que le groupe Anonymous et d'autres pirates informatiques malveillants pourraient développer très rapidement les capacités nécessaires pour avoir accès aux réseaux de systèmes de contrôle de processus et s'y introduire illégalement[31]. Dans certains cas, il semble évident que ce sont des États étrangers qui ont compromis des systèmes SCADA, mais d'autres incidents semblent être l'œuvre de pirates informatiques dont le seul but est d'étaler les compétences cybernétiques qui leur ont permis de prendre le contrôle de services clés.

Voici certains incidents liés au piratage informatique malveillant d'infrastructures essentielles survenus en 2011 et en 2012.

- Les infrastructures municipales de trois villes des États-Unis ont été compromises en 2011, dans ce que Michael Welch, sous-directeur adjoint de la division de cybersécurité du FBI, qualifie d'acte purement égocentrique d'un pirate informatique ayant pris le contrôle des systèmes essentiels d'une ville importante.

- Le système informatique de Stratfor, une entreprise d'analyse de renseignements et d'affaires internationales, a été piraté par la faction « AntiSec » d'Anonymous en décembre 2011. Des renseignements personnels sur environ 850 000 abonnés, comprenant prétendument

des responsables canadiens de la sécurité, des employés du service de renseignements britannique, des militaires, des policiers et des employés de l'OTAN, auraient été diffusés.

- On soupçonne des hacktivistes étrangers d'avoir attaqué les ordinateurs d'une compagnie de chemin de fer des États-Unis en décembre 2011. Selon la Transportation Security Administration, l'attaque a entraîné la perturbation des signaux ferroviaires, nuisant ainsi à la circulation ferroviaire dans le Nord-Ouest des États-Unis.

- En février 2012, des hacktivistes associés au groupe Anonymous ont intercepté une conversation téléphonique supposée être sécurisée entre le FBI et Scotland Yard qui était transmise par Internet et où les interlocuteurs discutaient d'une enquête conjointe portant sur la cybercriminalité. Anonymous a diffusé la conversation sur son site Web. La même journée, Anonymous a aussi temporairement désactivé la page d'accueil du site Web du DHS.

- À la mi-février 2012, Anonymous a annoncé qu'il était parvenu à désactiver le site Web du Central Intelligence Agency des États-Unis ainsi que ceux de l'État de l'Alabama et de la chambre des mines du Mexique.

///

*Quand les hacktivistes ont choisi une cible, ils semblent habituellement en mesure de compromettre l'intégrité de ses systèmes cybernétiques ou de technologie de l'information. Tout indique que les personnalités publiques, les gouvernements et les groupes industriels sont susceptibles d'être la cible, pour des raisons politiques ou idéologiques, d'attaques perturbant leurs systèmes cybernétiques, comme ce qui s'est produit pour Stratfor. Le plus souvent, les pirates informatiques malveillants s'adonnent à des attaques d'hameçonnage et à d'autres escroqueries, qui sont conçues pour extraire des données personnelles sur des personnes ou d'importants renseignements commerciaux exclusifs provenant d'organisations à des fins de vol d'identité et d'accès illégal à des systèmes cybernétiques sensibles.*

Les pirates informatiques et autres cyberguerriers inventent constamment de nouvelles techniques leur permettant de s'infiltrer dans certains systèmes. Il y a plusieurs mois, Anonymous a annoncé qu'il avait reproduit le code du célèbre virus Stuxnet, qui a été distribué sur Internet. Tandis que les attaques par déni de service distribué (DDoS) telles que celles perpétrées par Anonymous en 2011 gagnent en popularité, certains éléments laissent croire qu'elles deviendront plus complexes et efficaces en 2012, alors que les pirates passeront du niveau des réseaux à celui des applications et des opérations. L'outil #RefRef qu'Anonymous a publié en 2011 et qui exploite les vulnérabilités d'injection SQL servant à mener les attaques DDoS en est un exemple.

Selon McAfee Inc., encore plus d'interruptions numériques organisées par des hacktivistes malveillants se produiront en 2012, car de nombreux réseaux industriels et d'infrastructures nationales ne sont pas conçus pour la connectivité moderne, ce qui les rend particulièrement vulnérables. L'entreprise s'attend à ce que les pirates profitent de la situation en 2012, pas seulement pour faire du chantage ou de l'extorsion, mais, dans le pire des cas, pour interrompre des services publics comme l'alimentation en eau et en électricité[32]. On rapporte que même McAfee a été victime d'hacktivistes associés à Anonymous en janvier 2012.

Le Department of Homeland Security (DHS) des États-Unis a signalé une hausse rapide du nombre d'organisations privées demandant son aide pour protéger leurs systèmes de contrôle automatisé. Parfois, même des organisations sophistiquées ne se rendent pas compte qu'elles ont été victimes de piratage informatique et sont susceptibles de ne pas vouloir admettre que des données ont été compromises pour ne pas entacher leur réputation. Le général Keith Alexander, directeur de la National Security Agency (NSA), a récemment comparé les défenses actuelles des entreprises à la ligne Maginot, la ligne de fortifications construite par la France après la Première Guerre mondiale et qui n'a pas empêché la progression des Allemands pendant la Seconde Guerre mondiale. Il a mentionné que les entreprises ont établi un périmètre de défense et elles attendent. Il a indiqué que les entreprises et les fournisseurs de services Internet devraient plutôt chercher activement des « signatures » qui pourraient révéler la présence de nouveaux types d'attaques et qu'ils devraient ensuite les communiquer à ceux qui pourraient être touchés[33].

## MENACES INTERNES

Une menace interne est une attaque perpétrée par un membre du personnel d'une entreprise, d'une organisation responsable d'une infrastructure essentielle ou d'un ministère ou organisme du gouvernement, ou avec son aide. Les membres du personnel mécontents ou corrompus, ou encore ceux qui se sont infiltrés dans une organisation dans le but précis de mener une attaque contre elle ou de fournir à d'autres les renseignements leur permettant de le faire, représentent une menace importante et grandissante. Les agents d'infiltration sont des membres d'un groupe ou d'une organisation de renseignements étrangère hostile qui ont été choisis parce qu'ils ont les compétences, la motivation et les habiletés nécessaires pour endosser une identité leur permettant d'avoir accès à un emploi et à des renseignements sensibles ainsi qu'à des zones réservées d'une organisation en particulier.

Des menaces internes peuvent provenir d'employés mécontents ou faisant face à des difficultés financières, motivés par l'appât du gain, faisant du zèle religieux ou fortement en désaccord avec des politiques gouvernementales. Un facteur important favorisant la trahison à l'interne est la tendance à la restructuration organisationnelle, notamment la réduction et le réaménagement des effectifs, le remplacement de postes réguliers par des postes à temps partiel, et même les changements technologiques rapides. La trahison à l'interne pourrait également être motivée par un solide lien d'attache à une identité étrangère[34].

En dehors des véritables employés mécontents, les menaces internes proviennent aussi d'agents ou de taupes infiltrés dans des organisations importantes ciblées par des adversaires. La doctrine stratégique et la tactique opérationnelle d'al-Qaïda admettent le recrutement et le placement d'agents à des postes au sein de secteurs des infrastructures essentielles de pays ciblés[35]. Le groupe met particulièrement l'accent sur l'infiltration de services de police, des forces armées, de partis politiques, de médias, de groupes islamiques, de sociétés pétrolières, d'agences privées de sécurité et d'institutions civiles importantes. Des études récentes montrent que les agents qui s'infiltrent de cette façon peuvent présenter une menace plus importante que les employés mécontents[36]. Un adversaire infiltré est particulièrement difficile à déceler et à arrêter en raison de la nature délicate de la surveillance de sa propre main-d'œuvre ainsi que de l'indifférence et de la réticence naturelle des employés à dénoncer le comportement irrégulier ou suspect d'un collègue.

Dans un rapport publié en juillet 2011 par le DHS des États-Unis et intitulé *Insider Threat to Utilities*, on prévenait que des extrémistes violents sont effectivement parvenus à infiltrer des postes dans des services d'énergie des États Unis et qu'ils posaient une importante menace physique et cybernétique pour les infrastructures essentielles[37]. On y indique également que les renseignements confidentiels concernant des sites, des infrastructures, des réseaux et des employés sont précieux pour les adversaires et peuvent accroître les dommages causés par une attaque contre les infrastructures des services. Des États étrangers, notamment la Chine, ont également recruté des agents internes pour effectuer de l'espionnage économique dans des industries primaires et manufacturières de haute technologie.

Paradoxalement, les nouvelles technologies numériques qui ont rendu possibles l'agrégation, le stockage et la récupération rapide de données ont accentué la menace à la sécurité nationale. Elles ont facilité la tâche aux agents internes qui commettent des actes de sabotage industriel ou économique contre des services gouvernementaux et des infrastructures essentielles et ont créé de nouvelles occasions favorables. Des quantités énormes de données précieuses peuvent être téléchargées et transférées par Internet ou encore copiées subrepticement sur des dispositifs numériques miniatures et « exfiltrées » de l'organisation sans que personne ne s'en aperçoive. Les agents internes pourraient être en mesure d'obtenir un accès privilégié à des cybersystèmes qui analysent, surveillent et commandent des infrastructures, ou encore d'obtenir des renseignements révélant les vulnérabilités physiques et cybernétiques d'usines en écoutant des discussions non surveillées. La connaissance d'une entreprise et de ses systèmes donne à l'agent interne l'avantage d'être en mesure de comprendre des données qui seraient obscures pour un visiteur ou un intrus chanceux parvenant à franchir les barrières physiques de sécurité.

Les secteurs des infrastructures et les institutions de diverses administrations ayant été confrontés à des menaces internes provenant de membres de groupes djihadistes internationaux au cours des dernières années comprennent notamment des aéroports, des compagnies aériennes, des services d'énergie, des centrales nucléaires, des sociétés pétrolières, des laboratoires universitaires, des réseaux d'aqueduc, des ministères traitant des renseignements confidentiels ainsi que des services de sécurité du Danemark, des États-Unis, des Pays-Bas et du Royaume-Uni. On se préoccupe particulièrement des menaces grandissantes envers les aéroports (qui se distinguent des compagnies aériennes en soi) provenant de cas relevés dans diverses administrations où des employés

mécontents de boutiques hors taxes, de hangars de fret ou sur le terrain, des bagagistes et des fournisseurs de carburant ont été corrompus par des terroristes.

En Australie, un employé mécontent d'une usine d'épuration d'eau a truqué un système de contrôle informatisé et a déversé plus de 750 000 litres d'eaux usées dans des parcs, des ruisseaux et le terrain d'un hôtel Hyatt[38]. Dans un autre cas, un ancien garde de sécurité d'un hôpital de Dallas a récemment été reconnu coupable d'avoir corrompu des systèmes de contrôle de processus dans le but d'interrompre les systèmes de climatisation de son ancien lieu de travail. Il a été condamné à une peine d'emprisonnement de 110 mois en mars 2011.

# CHAPITRE 3
# RISQUES ET PROBABILITÉS QUE DES CYBERATTAQUES SOIENT LANCÉES

## LE CYBERESPACE : CARACTÉRISTIQUES ET PRÉOCCUPATIONS

La lutte contre les cybermenaces comporte certaines difficultés particulières, puisque par comparaison à d'autres secteurs, le cyberespace comporte certains éléments différents ou de plus et que ces éléments viennent compliquer la tâche lorsqu'il s'agit d'évaluer les probabilités et les risques d'une cyberattaque.

*La fréquence du changement*
Le cyberespace est un domaine axé sur la technologie et au sein duquel des innovations révolutionnaires peuvent apparaître en quelques jours à peine. Par conséquent, des menaces contre la sécurité peuvent survenir et évoluer à un rythme si rapide qu'elles parviendront à annuler l'effet habituel de balancier des avantages qui marque les cycles d'action-réaction des autres domaines. Selon l'entreprise de sécurité cybernétique McAfee, 60 000 nouvelles variantes de logiciel malveillant sont lancées presque chaque jour.

*Limites géographiques*
Puisque les infrastructures essentielles fonctionnent habituellement dans les marchés mondiaux, elles ont absolument besoin d'une connectivité à l'échelle internationale pour remplir leurs intérêts opérationnels. Étant donné qu'il n'existe pas de limites géographiques dans le cyberespace, les personnes, les groupes ou les États-nations attaquants peuvent être n'importe où; d'ailleurs, leurs objectifs sont habituellement sans limites. Dans le domaine du cyberespace, plus que dans tout autre, les lignes qui délimitaient les menaces nationales des menaces étrangères ont été brouillées, et la cueillette du renseignement de sécurité à l'échelle internationale ainsi que la création de relations de travail plus étroites avec les intervenants du secteur privé et avec les partenaires internationaux sont maintenant considérées comme des priorités. Les technologies cybernétiques tendent à estomper les séparations entre les organisations, et elles encouragent ces dernières à échanger des données plus librement, à adopter les mêmes processus et à utiliser les mêmes technologies.

*Anonymat et attribution*

En temps normal, l'analyse des menaces cybernétiques en fonction des cibles prévues, des méthodes et des moyens adoptés est possible. Cependant, il peut s'avérer plus difficile, voire impossible, de dégager les motifs d'attaques de grande envergure, la technique empruntée et l'identité de l'agresseur en raison de l'anonymat que confère cet environnement et de la rapidité à laquelle les menaces cybernétiques évoluent. Par comparaison aux menaces perpétrées dans d'autres domaines, il faudra surtout axer les efforts sur l'agresseur, particulièrement lorsque l'adversaire est agile et inventif et que la victime n'est soit pas consciente du danger, soit qu'elle a de la difficulté à comprendre les complexités relatives à l'environnement des menaces cybernétiques.

*Lois, règlements et autorités compétentes*

La protection des infrastructures essentielles dans le domaine en constante évolution des technologies de l'information et de la communication n'est pas de tout repos, et pour ce faire, les mesures législatives doivent être conçues d'une telle façon qu'elles peuvent évoluer au même rythme que la situation. Dans le domaine cybernétique, plus que dans tout autre domaine, l'application de règlements ou de contraintes et de mesures politiques de dissuasion efficaces est particulièrement difficile étant donné les enjeux relatifs à l'attribution, à la rapidité à laquelle les nouvelles menaces cybernétiques évoluent et à l'absence de frontières.

Les législateurs, les responsables de l'application de la loi et les personnes chargées de la réglementation, tant à l'échelle nationale qu'internationale, ont du mal à s'adapter aux nouvelles menaces cybernétiques; il n'y a pas assez de règles, de protocoles et de normes à cet égard, et ceux qui existent sont déconnectés et conflictuels. Ces problèmes sont d'ailleurs reflétés dans le titre d'un rapport récent du groupe de réflexion Security and Defence Agenda (SDA); *Cyber Security: The Vexed Question of Global Rules* qui, entre autres, insiste sur la nécessité d'élaborer des normes de sécurité internationales fondées sur les pratiques exemplaires[39].

Les mesures d'intervention mises en place par les États ont tendance à être rigides et fragmentées puisque les questions de compétence nuisent à l'adoption d'une démarche uniforme et holistique ayant trait aux activités cybernétiques à l'échelle nationale et mondiale. À ce jour, il n'existe toujours pas de définition convenue du concept de cyberattaque contre un pays ou de violation de la souveraineté. À l'échelle internationale, la possession fragmentée et le contrôle

réglementaire des infrastructures des technologies de l'information et de la communication figurent parmi les principaux problèmes à résoudre. Alors que dans un pays donné, des règlements stricts contre les cybercriminels sont édictés et appliqués, dans un autre pays dont les programmes sont moins développés, ces mêmes criminels pourraient s'adonner assez ouvertement à leurs activités.

Les propriétaires et exploitants des réseaux du secteur privé sur lesquels reposent les infrastructures essentielles comme les services publics, les systèmes de contrôle de la circulation aérienne, les banques et les fournisseurs d'alimentation en eau font de plus en plus appel aux organisations de sécurité et du renseignement pour coordonner des alertes et pour obtenir du renseignement sur la menace ainsi que des conseils sur les façons de se protéger contre le nombre croissant de virus, de vers et d'autres logiciels malveillants qui sont lancés. Pour répondre à ces besoins, ces organisations auront probablement à faire face à diverses contraintes, soit constitutionnelles, légales, de compétences et de ressources, et à des problèmes concernant la protection des sources et la responsabilité. Même si les deux côtés ont de bonnes raisons de ne pas vouloir divulguer l'information, vu la menace potentielle, des changements sont nécessaires. La vice présidente et agente principale des technologies du secteur public mondial à McAfee, Phyllis Schneck, estime que tant que les données ne seront pas mises en commun et que les gens et les machines n'auront pas tous les renseignements nécessaires, cela équivaut à une partie d'échec où seule la moitié des pièces est utilisée[40].

Aux États Unis, les lois ayant permis d'établir les services actuels du renseignement du pays sont maintenant les mêmes qui les empêchent d'échanger de l'information classifiée avec les entreprises du secteur privé. Cependant, la loi américaine intitulée *Cyber Intelligence Sharing and Protection Act* de 2011 figure parmi de nombreuses initiatives conçues pour aborder la question de la cybersécurité dans le secteur privé. Le sous-comité sur la Sécurité intérieure du Sénat américain a proposé un projet de loi exigeant du DHS qu'il élabore des normes sur la cybersécurité et qu'il collabore avec l'industrie afin de s'assurer que ces normes soient bel et bien appliquées.

*Perspectives éthiques*

L'identification de l'agresseur cybernétique ou l'analyse des attaques en vue d'en dégager les motifs et les techniques comportent souvent certaines difficultés qui, elles, ont des répercussions sur les évaluations des menaces et des risques ainsi que sur le volet éthique des interventions de sécurité mises en place. Au

départ, une cyberattaque pourrait être considérée comme étant moins grave qu'une attaque physique puisqu'elle ne met pas immédiatement la vie en danger. Cependant, il est faux de penser ainsi, puisqu'une attaque majeure visant à perturber le réseau électrique ou à dévier les systèmes d'alimentation en eau pourrait entraîner des décès et causer de la souffrance humaine considérable.

Il ne sera pas facile de trouver un cadre commun d'éthique, de normes et de valeurs pouvant être appliqué tant aux agresseurs qu'aux défenseurs engagés dans un conflit cybernétique. Les auteurs d'une attaque pourraient très bien considérer comme étant des mesures préventives et *défensives* un logiciel implanté leur permettant de neutraliser ou d'endommager l'équipement ou les chaînes d'approvisionnement de services d'adversaires potentiels en cas de conflit. Les défenseurs, par contre, verront très probablement de telles mesures comme étant *offensives* et un signe que des intentions malveillantes sont à prévoir. Après que des djihadistes aient lancé des offensives cybernétiques à répétition contre les sites Web d'Israël, les autorités israéliennes ont affirmé que leurs réponses aux attaques cybernétiques seraient les mêmes que celles déployées en cas d'actes terroristes.

Dans le monde virtuel, la façon dont sont modélisées les normes sociales n'est pas encore bien comprise, ce qui nuit à notre capacité de dissuader ou de motiver les divers intervenants. Il sera difficile de déterminer et de définir les règles d'engagement appropriées pour les cas d'espionnage d'État et industriel. Il sera surtout difficile de situer la faille dans la ligne qui sépare l'entreprise privée de l'entreprise publique, ou de décider dans quelle mesure les mouvements des pirates informatiques activistes devraient être considérés comme une expression numérique légitime de la désobéissance civile. Pour dégager les défis à surmonter et trouver des solutions, la pleine compréhension des motifs humains est requise, mais elle n'est possible que grâce à des recherches et des discussions plus poussées.

L'opposition aux initiatives visant à accroître la cybersécurité est habituellement ancrée dans des préoccupations et des attentes relatives à l'équilibre entre la sécurité et la protection de la vie privée. Il semblerait donc que les prochaines étapes devront surtout être axées sur l'amélioration des capacités d'attribution, de façon à faciliter et à justifier les mesures prises contre les pirates informatiques tout en réduisant sélectivement l'anonymat sans pour autant contrevenir aux lois protégeant la vie privée des gens.

## NOUVELLES MENACES

Le cyberespace peut servir de point de départ à petit prix et à faible risque au sein duquel un attaquant souhaitant se mesurer à un adversaire plus fort que lui dans un environnement asymétrique pourra lancer diverses opérations nuisibles et destructrices, ainsi que recueillir des renseignements. Des acteurs ne jouant qu'un rôle secondaire peuvent exercer une très grande influence dans le milieu cybernétique, puisque ce milieu est maintenant devenu un espace multidimensionnel d'attaque où des auteurs d'attaques peuvent cibler des infrastructures essentielles à distance sans devoir être exposés physiquement à des forces défensives. Les méthodes physiques habituelles de protection des infrastructures essentielles ne sont plus suffisantes, et le Canada ne peut plus se contenter d'adopter une position réactive et défensive qui a longtemps caractérisé les mesures de protection de la sécurité.

Les techniques et les technologies offensives ont évolué rapidement au cours des vingt dernières années, ce qui a ainsi donné lieu à la création de nouvelles menaces plus complexes possibles grâce à l'amélioration des compétences des pirates informatiques et à la technologie à la fine pointe à laquelle ils ont maintenant accès. Les infrastructures essentielles informatiques sont non seulement vulnérables à la pénétration et à l'exploitation par des réseaux de communication, mais leurs systèmes de commandes et de contrôle sont aussi susceptibles d'être infectées, ce qui pourrait entraîner leur destruction physique. Cette possibilité a été démontrée avec la découverte, en 2010, du ver informatique Stuxnet, le premier ver conçu précisément pour contrecarrer les processus de contrôle des systèmes industriels. Cette nouvelle arme destructrice avait été créée pour passer de l'environnement numérique au monde physique pendant une attaque directe, elle n'avait pas besoin d'une connexion Internet et elle avait le potentiel de perturber des gouvernements, des organisations et des infrastructures essentielles partout dans le monde.

Alors que les systèmes de contrôle fonctionnaient habituellement à partir d'un ensemble de connexions en série ou par modem, soit directes ou par radio, la tendance actuelle selon laquelle on lie les divers SCADA et réseaux des bureaux centraux à l'aide d'une connexion Internet a contribué à augmenter la vulnérabilité des systèmes et le risque d'incidents en cascade dans les divers secteurs des infrastructures essentielles. Le bureau national de coordination de la lutte contre le terrorisme des Pays Bas a émis un avertissement expliquant qu'il est très probable qu'un logiciel malveillant semblable au ver Stuxnet soit

recréé par des adversaires afin de lancer des cyberattaques contre des systèmes d'infrastructures essentielles vulnérables[41].

De plus, la complexité accrue des systèmes de technologie de l'information a également contribué à l'augmentation de la possibilité que de vulnérabilités pouvant être exploitées soient créées par accident, ou encore qu'il soit plus facile de dissimuler l'introduction délibérée de vulnérabilités. Dans la même veine, il devient de plus en plus difficile, pour le nombre limité d'experts dignes de confiance, de vérifier l'intégrité des systèmes. Alors que le rapport de SDA sur la cybersécurité insiste sur la nécessité de remédier à la pénurie de personnel qualifié en matière de cybersécurité pour lutter contre les menaces cybernétiques, un rapport de l'Intelligence and National Security Alliance met l'accent sur le fait que les pirates informatiques n'ont ni besoin de nombreuses ressources, ni d'être éduqués.

En outre, de nombreux pays de l'Ouest impartissent à de tierces parties, souvent établies dans des pays en développement, les tâches relatives à la conception, à la création et à l'entretien de la technologie de l'information de tous les secteurs. Bien que l'impartition et l'utilisation de technologies ordinaires et disponibles en magasin soient fondées sur des principes économiques, il y a tout de même des risques inhérents de sécurité qui ne sont pas tenus en compte dans le marché.

Les mêmes arguments pourraient s'appliquer au concept de l'infonuagique (cloud computing) et aux vastes centres de fusion des données. La circulation rapide de données que caractérise l'infonuagique, ainsi que l'archivage massif de données en un seul site soulèvent d'autres préoccupations quant à la sécurité dans Internet en ce qui a trait à l'emplacement des nuages de données et à leur vulnérabilité potentielle aux pirates informatiques, à l'espionnage ou à la divulgation accidentelle. Par exemple, un tiers des installations d'infonuagique de Google sont situées au Canada. Le fait de déplacer et d'archiver une concentration de données dans des sites dont la sécurité n'a pas vraiment été vérifiée et dont les vulnérabilités sont encore incertaines pourrait exposer l'information personnelle, industrielle et même gouvernementale de nature délicate à des risques potentiels et ayant d'importantes répercussions pour la sécurité nationale[42].

Lors de sa comparution devant le comité spécial sur le renseignement du Sénat américain en janvier 2012, le directeur du Federal Bureau of Investigation des États Unis a affirmé que les menaces de cyberespionnage, de crimes

informatiques et d'attaques contre les infrastructures essentielles surpasseront le terrorisme au titre de menace principale à laquelle le pays devra faire face. Dans ce cas, les répercussions accrues de ces cybermenaces trouveront probablement écho au Canada.

(L'annexe A donne plus de détails sur le secteur des technologies de l'information et des communications.)

## ÉVALUER LES RISQUES ET LES VULNÉRABILITÉS

La tenue d'évaluations des menaces et des risques est un processus complexe. La complexité structurelle de la menace doit être bien comprise et elle doit être prise en compte dans l'évaluation, ce qui est particulièrement difficile à faire lorsqu'il s'agit de menaces terroristes ou lorsque des infrastructures essentielles nationales sont la cible d'attaques cybernétiques malveillantes. Les fournisseurs de produits de sécurité du secteur privé ont des intérêts commerciaux à défendre, et ces intérêts ne tiennent pas compte des besoins et des stratégies du secteur public. Aussi, dans les entités commerciales et ministérielles, les victimes de la cybercriminalité hésitent à révéler le fait que leurs réseaux ont été compromis (s'ils en sont conscients). De plus, ces éléments qui nuisent à l'exécution d'évaluations réalistes des menaces et des vulnérabilités sont exacerbés par la question des coûts de sécurité, que nous examinerons sous peu.

Les gestionnaires des infrastructures essentielles doivent avoir une méthode fiable d'évaluation des risques pour décider des mesures de sécurité requises dans leurs installations. Les risques sont habituellement évalués selon la méthode actuarielle, qui tient compte du relevé des menaces, des vulnérabilités connues et des pertes réelles. Cependant, de nombreux nouveaux risques n'ont aucun précédent et, par conséquent, ils ne peuvent pas être déterminés à l'aide de méthodes actuarielles conventionnelles. Par conséquent, ils sont considérés comme étant des « risques pernicieux », justement parce qu'ils ne peuvent pas être évalués à l'aide de méthodes actuarielles et parce qu'une évaluation de la probabilité que la menace se concrétise doit être effectuée. Dans ce cas, il faut faire preuve d'un jugement analytique minutieux fondé sur une compréhension approfondie des participants possibles, de la complexité de leur organisation, de leurs systèmes de croyances, des tendances idéologiques et des tendances cognitives et comportementales, des doctrines tactiques et des objectifs opérationnels.

Dans ses travaux d'avant garde sur les « risques pernicieux », Nancy Hayden du National Laboratories de Sandia caractérise le terrorisme en tant que phénomène complexe d'interaction dynamique de nature sociale, technologique et institutionnelle.[43] Certains modèles actuariels récemment élaborés dans les laboratoires nationaux américains et par des entreprises spécialisées dans la modélisation des risques ont entrepris diverses mesures visant à tenir compte des « risques pernicieux » dans leurs évaluations des probabilités (un certain nombre de ces modèles sont énoncés à l'annexe B).

# CHAPITRE 4
# CONTRER LES CYBERMENACES – UNE APPROCHE DE PARTENARIAT EN MATIÈRE DE PROTECTION DES INFRASTRUCTURES ESSENTIELLES

En raison de la rapidité des changements technologiques en matière d'information et de communication, le gouvernement canadien n'est pas le seul à arriver à la conclusion que les défenses actuelles ne permettront pas d'assurer l'intégrité et la disponibilité de ses systèmes d'information de façon efficace ni d'empêcher la destruction ou l'arrêt des infrastructures essentielles. La perception de plus en plus répandue que les menaces et les vulnérabilités sont croissantes, a poussé les décideurs d'un certain nombre d'administrations à envisager des moyens d'améliorer la sécurité des réseaux, de renforcer leur résilience et d'empêcher les terroristes et autres pirates informatiques de compromettre la sécurité et la compétitivité sociétales et de s'attaquer aux infrastructures essentielles. Alors que la plus grande partie des incidents cybernétiques signalés découlent des activités exercées, qui étaient considérées jusqu'à maintenant comme représentant une moins grande menace, les préoccupations croissantes des É.-U. au sujet de la stratégie de la Chine, qui développe son économie en subtilisant des technologies, ont provoqué une levée de boucliers en faveur d'une réponse plus concrète.

Étant donné que la menace découle de la nature même des technologies numériques, on demande généralement aux spécialistes en informatique de répondre à la menace; si la sécurité de l'information est perçue comme étant un problème technique, des solutions proposées seront axées sur l'identification des vulnérabilités dans les systèmes informatiques d'une organisation et sur la proposition de solutions techniques — la plupart d'entre elles seront identifiées et mises en œuvre sur le marché privé. Les niveaux de protection technique tiennent compte de nombreuses questions, mais le principal moyen de tenter de renforcer la résilience consiste à investir dans les systèmes de sauvegarde, la redondance, l'isolement des systèmes et autres mesures.

Alors que la question de la sécurité de l'information s'est posée en raison des changements technologiques, on reconnaît de plus en plus que le problème ne peut pas être traité uniquement au niveau technique des opérations, mais qu'il faut plutôt adopter une approche plus globale à l'échelon national. Le défi consiste maintenant *à assurer la protection d'une société axée sur l'information en général* plutôt qu'à protéger les infrastructures de l'information. Outre

la stimulation de l'investissement dans des technologies de défense, cette approche ferait appel à une initiative de cybersécurité proactive de la part des services du renseignement de façon à *prévenir* les contaminations plutôt qu'à simplement y réagir. Cette initiative mettrait davantage l'accent sur la lutte contre les activités cybernétiques qui visent à percer les secrets du gouvernement et des entreprises représentante une plus grande menace à la sécurité nationale que les cyberattaques massives qui endommagent ou perturbent les systèmes informatiques. Un des principaux objectifs de la stratégie de cybersécurité des É.-U. S. consiste à prévenir le vol de propriété intellectuelle commis au moyen du cyberespionnage. Il s'agit également d'une responsabilité essentielle pour le milieu de la sécurité et du renseignement au Canada.

La sécurité nationale est la prérogative de l'*État*, mais au Canada ce sont les propriétaires et exploitants d'infrastructures essentielles qui sont les principaux responsables de la sécurité et de la protection de leurs actifs. Les organisations du secteur privé peuvent s'assurer contre les risques tant actuariels que ceux liés au terrorisme, mais la plupart du temps, les cadres supérieurs tendent à considérer que la sécurité est une source de complications et une charge indésirable à assumer pour exercer des activités, qu'il faut diminuer. Selon un sondage international,[44] l'imprévoyance, si ce n'est l'apathie, prévaut habituellement dans de nombreux bureaux de cadres supérieurs, particulièrement en ce qui concerne les menaces cybernétiques et terroristes. Les agents de sécurité ont rarement accès à la haute direction. En réalité, nous avons recensé un certain nombre de cas où des hauts dirigeants ont réellement refusé d'entendre parler d'évaluations des menaces de la part de leur propre personnel de sécurité de peur de devoir assumer des obligations à cet égard.

Le coût financier visant à assurer la sécurité de leurs infrastructures essentielles contre les cyberattaques est une considération importante pour les propriétaires et les exploitants. Ce fardeau lié aux coûts peut comprendre des dépenses engagées pour des redondances intégrées, des solutions logicielles et matérielles, le recours à des spécialistes en dotation et la formation professionnelle, de même que la planification de mesures d'urgence. Alors qu'il appartient clairement aux propriétaires et exploitants d'assurer la protection de leurs infrastructures essentielles contre les menaces criminelles, qui est prise en compte dans les coûts opérationnels, les menaces liées à la sécurité nationale ont des ramifications qui vont au-delà du domaine privé et qui ont aussi une incidence sur le public.

Par conséquent, il semblerait approprié que les coûts liés à la protection des infrastructures essentielles contre certaines menaces à la sécurité nationale soient assumés proportionnellement par toutes les parties qui bénéficient de cette protection. Une certaine aide financière du gouvernement central accordée aux propriétaires et exploitants d'infrastructures essentielles pour qu'ils tiennent compte des risques à faible probabilité, mais aux conséquences considérables, permettrait de défendre plus efficacement non seulement les intérêts commerciaux des propriétaires et exploitants d'infrastructures essentielles, mais aussi ceux du grand public et de renforcer sa confiance en la capacité du gouvernement de maintenir les services essentiels en cas de crise.

Le Cyberspace Strategic Plan des États-Unis vise à renforcer la résilience en matière de cybersécurité grâce à une technologique qui favorise le développement de logiciels sécurisés; l'instauration d'incitatifs économiques comme des interventions commerciales, juridiques, réglementaires ou institutionnelles; de même que l'élaboration de stratégies visant à aider les professionnels de la sécurité à faire en sorte qu'il soit plus coûteux et plus difficile pour les pirates informatiques de passer à l'acte [45]. S'il est adopté l'an prochain, le nouveau projet de loi sur la cybersécurité, présenté récemment au Congrès, énoncerait que le DHS est l'organisme responsable de la protection des réseaux tant gouvernementaux que privés et demanderait aux exploitants d'infrastructures d'élaborer un plan sur la cybersécurité et de le présenter au DHS pour approbation.

## ALLER DE L'AVANT : LE RÔLE DU RENSEIGNEMENT

La cybersécurité est généralement considérée comme un élément essentiellement défensif de protection des ressources numériques, axée tout particulièrement sur des solutions techniques. Une position défensive est passive et réactive, du point de vue de la procédure, et elle accusera toujours un retard par rapport aux menaces émergentes. Les adversaires ont toujours l'initiative. En conséquence, la protection des infrastructures essentielles et des systèmes d'information contre les cybermenaces est rapidement repensée, de nos jours, comme la défense d'une société fondée sur l'information, dans son ensemble; il s'agit d'une considération de sécurité nationale. Et en matière de sécurité nationale comme de guerre, la meilleure défense s'appuie sur une attaque dynamique. En allant plus loin que les solutions purement défensives et techniques, une approche proactive en matière de protection des infrastructures essentielles contre les cybermenaces devra s'appuyer sur les capacités et les ressources du renseignement pour prévenir les attaques en repérant et en anticipant les menaces éventuelles.

La nouvelle stratégie de lutte contre le terrorisme du Canada, introduit un élément visant explicitement à priver les terroristes de l'accès à des moyens d'action en vue de réduire les vulnérabilités en matière de cybersécurité, entre autres, au moyen de mesures proactives[46]. Une évaluation des capacités actuelles et futures des adversaires constitue un exemple patent de cette façon de faire. Alors que les États-Unis ont également montré qu'ils étaient capables de réaliser des cyberattaques pour briser ou détruire le système informatique d'un ennemi, l'intérêt immédiat du Canada relativement à la sécurité nationale consiste à faire campagne de façon efficace et convaincante contre les cyberattaques perpétrées par les terroristes et les États étrangers en vue de miner leurs capacités à cet égard.

Au Royaume-Uni, le Centre for the Protection of National Infrastructure (CPNI) travaille en étroite collaboration avec les autres organismes centraux pour conseiller les entreprises et les organisations de tous les secteurs des infrastructures essentielles du pays, ainsi que pour aider à réduire les risques et la vulnérabilité à l'égard des cybermenaces. Il diffuse également des avertissements et des alertes, et il offre de l'assistance pour résoudre les incidents graves en matière de TI. Le CPNI fait partie des services de sécurité du Royaume-Uni.

Mike McConnell, ancien directeur de l'organisme de renseignements national des États Unis, a récemment commenté les capacités uniques des organismes du renseignement américains qui peuvent contribuer à la protection des entreprises

américaines contre le cyberespionnage et les cyberattaques. Le principal enjeu consiste à déterminer comment on peut tirer profit de cette capacité et l'offrir au secteur privé afin de protéger les infrastructures essentielles.

Même si les États-Unis s'affairent à établir des capacités renforcées et proactives en matière de cybersécurité, la priorité devrait être accordée, selon McConnell, à protéger les infrastructures essentielles du pays contre les cyberattaques, par exemple le secteur financier, le réseau électrique et le système de transports, de même qu'à empêcher le vol de la propriété intellectuelle au moyen du cyberespionnage. Ces craintes sont similaires à celles du Canada. Un nouveau projet de loi sur la cybersécurité approuvé par le Intelligence Committee de la Chambre des représentants des États Unis en décembre 2011 permettrait aux organismes du renseignement américains d'échanger de l'information sur les cybermenaces avec les entreprises privées. Puisque c'est le gouvernement qui a accès aux données du renseignement sur les menaces, mais que ce sont les intervenants du secteur privé qui doivent assumer la responsabilité de la protection des ressources essentielles, il faut trouver certains arrangements qui permettent l'intégration de ces deux rôles. Bien souvent, les propriétaires et les exploitants d'infrastructures essentielles sont les premiers au courant de l'apparition de nouveaux virus ou vers informatiques. Il est donc essentiel de mettre en place un processus formel de collecte, d'analyse et de diffusion des données relatives aux cyberincidents d'importance.

La détection des menaces requiert, comme le précise la nouvelle stratégie antiterroriste du Canada, « de grandes capacités en matière de renseignements et une juste compréhension des facteurs stratégiques liés au contexte de la menace, de même qu'une collaboration étroite et des échanges fructueux de renseignements avec les partenaires tant au pays qu'à l'étranger[47] ». Le milieu de la sécurité et du renseignement du Canada possède un mandat unique, soit utiliser son accès à de l'information sensible sur la menace ainsi que ses capacités et son expérience en matière de capacités analytiques et opérationnelles pour agir dans l'intérêt de la sécurité nationale. Les renseignements d'origine électromagnétiques jouent également un rôle central dans la détection des menaces immédiates. Les efforts combinés en vue de protéger les réseaux d'information du Canada contre les intrusions sont réalisés grâce à un partenariat collaboratif qui permet une direction conjointe des enquêtes en vue de favoriser la détection, le repérage et les opérations préventives à l'égard des pirates potentiels, y compris les personnes à l'interne.

En plus de ces compétences de base et de ces capacités opérationnelles, les services du renseignement du Canada disposent d'autres moyens pour permettre une intervention solide et proactive en matière de sécurité nationale à l'égard des cybermenaces. L'échange d'information déjà en place avec les intervenants des infrastructures essentielles (lorsqu'il est indiqué de le faire) peut être amélioré par l'établissement de partenariats efficaces d'acquisition des connaissances, ce qui pourrait consolider la collaboration entre les secteurs public et privé en matière de cybersécurité. Les services du renseignement possèdent la crédibilité et la compétence nécessaires pour remplir ces rôles en raison de leur accès à l'information sur la menace, à leur expertise technique et analytique ainsi qu'à leur expérience en matière d'enquête.

Les intervenants des infrastructures essentielles de plusieurs secteurs du Canada (énergie et services publics, finances, technologies de l'information et de la communication et transports) se sont habitués à gérer à l'échelle locale les risques qui pèsent contre leurs installations. Néanmoins, il est notoire parmi les intervenants de ces secteurs importants que leurs défenses contre les menaces actuelles souffrent de faiblesses et de lacunes. Une approche fondée sur un partenariat global et bien rodé entre le secteur privé et le milieu de la sécurité et du renseignement est nécessaire pour aider les intervenants, de même que les autorités locales, à neutraliser ces vulnérabilités, à réduire les dommages possibles et à prévoir des mesures de résilience.

Les prérequis en matière de formation constituent un aspect souvent négligé de l'approche fondée sur le renseignement en matière de protection des infrastructures essentielles (y compris la cybersécurité). Le récent rapport de SDA intitulé *Cyber Security: The Vexed Question of Global Rules* a fait valoir que le manque de compétences en cybersécurité empêchait les organisations du secteur privé de recruter du personnel pour satisfaire à leurs besoins de sécurité[48]. Une formation et des qualifications spécialisées sont nécessaires pour préparer les agents de sécurité des entreprises à traiter, à protéger et à utiliser des documents fondés sur des données du renseignement. De même, les gestionnaires et les analystes du renseignement doivent posséder les compétences requises pour comprendre les menaces, les vulnérabilités et les interdépendances relatives aux processus et aux des secteurs industriels particuliers, de même que les caractéristiques et les besoins organisationnels qui y sont associés. Sans cette formation et en l'absence de gestionnaires et d'intervenants qualifiés en matière de sécurité, aucune tactique et aucune défense ne peut être complètement efficace.

Une approche proactive du renseignement en matière de cybersécurité des infrastructures essentielles devrait posséder les caractéristiques suivantes :

- Les objectifs opérationnels consisteraient à détecter et à prévenir les cybermenaces contre les infrastructures essentielles et la sécurité publique.

- Les activités de cybersécurité viseraient à repérer les menaces contre les infrastructures essentielles et à recueillir, analyser et diffuser l'information connexe, et ce, de façon systématique.

- Les données du renseignement devraient être rendues disponibles sur une base de « besoin de diffuser » entre les partenaires des milieux de la sécurité, du renseignement et de l'application de la loi. On s'attend à ce que les propriétaires et exploitants de ressources liées aux infrastructures essentielles du secteur privé communiquent leurs évaluations des vulnérabilités et des menaces aux services du renseignement et aux responsables de la sécurité, et qu'ils signalent toute compromission de leur réseau. Cette information serait protégée sur une base classifiée.

- Des renseignements exploitables sur les cybermenaces contre les infrastructures essentielles seraient diffusés au personnel ayant reçu leur certification de sécurité de certaines installations ciblées du secteur privé.

- Une capacité de réaction rapide est nécessaire en vue de réduire les conséquences des attaques, de prévenir toute aggravation et de tirer des leçons dans le but de mettre en place des pratiques exemplaires.

Peu importe la provenance des cybermenaces (terrorisme international, espionnage commandité par les États ou hacktivistes malveillants), toute attaque contre les infrastructures essentielles peut représenter une menace contre la sécurité nationale et la sécurité publique du Canada. Les capacités du renseignement devraient être déployées afin d'empêcher que les infrastructures essentielles soient prises pour cible, de détecter lorsque c'est le cas et de s'assurer que les auteurs sont poursuivis. Une intervention coordonnée fondée sur le renseignement face aux cybermenaces peut contribuer à empêcher les intrusions dans les installations névralgiques et les systèmes de technologie de l'information et de communication ainsi qu'à réduire les dommages résiduels.

Le renseignement fait partie intégrante du processus de prises de décisions à l'échelle tactique et stratégique. Dans le monde cybernétique, le renseignement peut accroître la capacité des gouvernements et des intervenants à évaluer les effets d'une cyberattaque, à réduire les risques et à intégrer la cybersécurité dans un processus efficace (y compris sur le plan économique) fondé sur des décisions éclairées. Un rapport de 2011 rédigé par le Cyber Council de l'Intelligence and National Security Alliance (INSA), intitulé *Cyber Intelligence: Setting the Landscape for an Emerging Discipline*, débute par une proposition selon laquelle [traduction] « même s'il est difficile d'évaluer clairement l'incidence réelle d'une cyberattaque, le coût est suffisamment important pour nécessiter la mise en place de mesures de cybersécurité appuyées par des données approfondies du renseignement cybernétique »[49]. Les données du renseignement relatives à la cybersécurité au sein des ressources des infrastructures essentielles devraient viser à faire en sorte que le coût soit élevé pour les adversaires qui tentent d'exploiter les vulnérabilités du système, que les chances de succès soient minimales, que les dommages probables soient atténués et que l'industrie et la société disposent des mesures de résilience adéquates.

# ANNEXE A
# DYNAMIQUES STRUCTURELLES DU SECTEUR DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Le secteur de l'infrastructure des technologies de l'information et de la communication englobe la téléphonie, la radiodiffusion et la télédiffusion, la connectivité Internet, les contrôles de l'accès au périmètre ainsi que la surveillance et le contrôle des satellites. Dans un environnement concurrentiel à l'échelle mondiale, les propriétaires et exploitants canadiens d'infrastructures essentielles, tout comme leurs homologues partout ailleurs, ont de plus en plus tendance à mettre en œuvre des cybertechnologies sophistiquées.

Parmi ces nouvelles technologies, mentionnons les systèmes de contrôle informatisés qui sont utilisés par bon nombre d'industries et d'infrastructures essentielles canadiennes pour surveiller et contrôler les processus délicats et les fonctions physiques. Ils exécutent des fonctions essentielles au sein des secteurs des infrastructures essentielles, notamment la production, le transport et la distribution d'électricité, le raffinage du pétrole et du gaz, les oléoducs, le traitement et la distribution d'eau, ainsi que les systèmes ferroviaires et de transport en commun.

De façon générale, les systèmes de contrôle recueillent les mesures des capteurs et les données opérationnelles sur le terrain, puis ils traitent et affichent cette information pour ensuite retransmettre des commandes de contrôle à l'équipement local ou à distance. Dans l'industrie de l'énergie électrique, les systèmes de contrôle peuvent gérer et contrôler la production, le transport et la distribution d'électricité, par exemple en ouvrant et en fermant les disjoncteurs et en établissant des limites pour les mises à l'arrêt préventives. Comme elle utilise des systèmes de contrôle intégrés, l'industrie du pétrole et du gaz peut contrôler les activités de raffinage dans une usine de traitement, surveiller à distance la pression et le flux des oléoducs troués et contrôler le flux de gaz naturel et les parcours du transport de gaz naturel. Les services publics d'eau permettent de surveiller efficacement à distance les niveaux des puits et de contrôler les pompes, le flux, les niveaux des réservoirs ou la pression dans les réservoirs de stockage, de surveiller les caractéristiques liées à la qualité de l'eau et de contrôler l'ajout de produits chimiques. Les systèmes de contrôle exécutent

des fonctions à la fois simples et complexes; ils permettent par exemple de surveiller les conditions environnementales dans un bureau particulier et de gérer la plupart des activités menées dans une centrale nucléaire.

Il existe deux principaux types de systèmes de contrôle : les systèmes de contrôle répartis (SCR), qui sont habituellement utilisés dans une seule centrale ou usine de traitement, ou dans une petite région géographique, et les systèmes d'acquisition et de contrôle des données (SCADA), qui sont utilisés pour mener de vastes activités de distribution géographiquement dispersées. À titre d'exemple, une société de service public pourrait utiliser un SCR pour produire de l'électricité et un système SCADA pour la distribuer.

La vulnérabilité des communications par Internet pose des risques importants aux infrastructures essentielles et aux activités qu'elles mènent. Par le passé, le matériel breveté, les logiciels et les protocoles de réseaux rendaient difficile la compréhension de la façon dont les systèmes de contrôle fonctionnent et la façon de les pirater; de nos jours, la volonté de réduire les coûts et d'accroître le rendement a poussé les organisations à mettre en œuvre des technologies normalisées et des protocoles de réseaux communs utilisés par les applications Internet. Les technologies normalisées largement utilisées ont des vulnérabilités bien connues, ce qui fait en sorte qu'un plus grand nombre de systèmes sont susceptibles de lancer des attaques, au moment où la disponibilité des outils d'exploitation sophistiqués et efficaces qui sont relativement faciles à utiliser a fait augmenter le nombre de personnes ayant les connaissances nécessaires pour lancer des attaques. L'augmentation de la connectivité de ces systèmes de contrôle avec d'autres, l'insécurité des cyberconnexions à distance et la grande disponibilité de l'information technique concernant les systèmes de contrôle ont contribué à accroître les risques de cyberattaques.

Les TIC sont utilisées dans le secteur du transport pour les réservations des voyageurs aériens, le contrôle relatif à l'embarquement et la gestion de la cargaison aérienne. Elles font également partie des programmes Expéditions rapides et sécuritaires et Pre-arrival Processing System (système PAPS), qui facilitent les autorisations préalables à la frontière pour les camions. Les systèmes de TIC connectés à Internet sont utilisés dans le secteur des finances pour les comptes clients (GAB), les appareils de paiement par cartes de débit ou de crédit et les virements de fonds.

Les systèmes SCADA et les TIC connexes sont intrinsèquement vulnérables à deux cybermenaces distinctes : 1) un accès non autorisé à des logiciels de contrôle, ce qui permettrait de prendre en charge le fonctionnement de l'infrastructure hôte et 2) l'insertion d'un paquet malveillant dans l'infrastructure hébergeant l'appareil SCADA à des fins d'espionnage ou de sabotage éventuel. Même si les systèmes de contrôle utilisent généralement une combinaison de branchement radio et sériel direct ou de branchement par modem, la tendance actuelle veut que la connectivité Internet entre les systèmes SCADA et les réseaux centraux des bureaux crée des vulnérabilités potentielles aux cyberattaques. Celles-ci peuvent compromettre ou endommager directement l'infrastructure concernée, en plus d'avoir une incidence profonde sur la société en raison des interdépendances.

Les TIC sont intrinsèquement vulnérables à la cyberinfiltration, généralement au moyen d'Internet, à des fins telles que l'accès à des renseignements de nature délicate et l'extraction de ces derniers, le traitement ou le détournement de flux de données, ou l'interférence relativement à des systèmes SCADA et à d'autres systèmes de contrôle industriels. L'infrastructure Internet est pour sa part plutôt robuste et présente des redondances. À l'heure actuelle (fevrier 2012), rien ne prouve la présence de cyberattaques hostiles ayant pour cible la communauté des services Internet.

Les secteurs et les systèmes des infrastructures essentielles dépendent de plus en plus des systèmes de positionnement global (GPS) par satellite en ce qui concerne le positionnement, la navigation et la synchronisation (PNS). Toutefois, même si les GPS sont considérés comme des systèmes extrêmement précis, très robustes et fiables, leurs signaux de PNS sont vulnérables aux perturbations liées à des phénomènes naturels comme les conditions météorologiques dans l'espace et l'interférence malveillante.

Les données et le logiciel nécessaire pour traiter ces données sont le plus souvent conservés dans de grands centres de données, des installations qui font des demandes importantes au réseau d'électricité. Même si ces technologies facilitent les activités commerciales et celles du gouvernement, elles sont aussi des cibles intéressantes pour les criminels et d'autres auteurs malveillants. Brandon Wales, directeur du Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) du DHS des États-Unis, estime que la dépendance généralisée aux GPS par satellite pour les services de positionnement, de navigation et de synchronisation (PNS) pose un risque unique en matière de cybersécurité. Les

incidents liés à l'interférence des GPS seraient en hausse. On a entre autres essayé de brouiller les signaux de l'aéroport international Newark Liberty, au New Jersey, au début de l'an 2010 : le système de renforcement au sol (GBAS), qui fournit les données GPS sur les arrivées et les départs d'avions, a été la cible d'une attaque.

Le mouvement rapide des données qui est un aspect de l'infonuagique soulève des préoccupations concernant la sécurité sur Internet en ce qui a trait à l'endroit où se trouvent les données issues de l'infonuagique et la mesure dans laquelle elles sont vulnérables aux pirates informatiques, à l'espionnage ou à la divulgation accidentelle. Le recours à l'infonuagique devrait augmenter; on s'attend donc à ce qu'il représente, d'ici 2015, près de 34 % du trafic dans les centres de données du monde entier, c'est-à-dire les immenses stations informatiques qui traitent et distribuent maintenant la majorité de l'information sur Internet. Ces centres de données représentent des catalyseurs encore plus grands pour le trafic Internet, en tant que moteurs numériques pour les services Internet les plus utilisés : Google, Facebook, Amazon, le service iCloud d'Apple et bien d'autres. Le tiers des systèmes d'infonuagique de Google se situe au Canada, ce qui peut avoir une incidence profonde sur la sécurité nationale. Au début de 2012, les systèmes d'infonuagique ont également été mis en œuvre pour les plateformes de gestion des catastrophes afin de permettre aux utilisateurs (premiers intervenants, gouvernements, organismes de secours, bénévoles et résidants locaux) d'avoir accès à l'information ainsi que de communiquer et de collaborer entre eux en temps réel par tous les types d'appareils informatiques, y compris les appareils portatifs, comme les téléphones intelligents, les assistants numériques et les tablettes iPad.

Le secteur des TIC a fait l'objet de changements rapides : la plupart des organisations dépendent d'Internet pour avoir accès à des données de gestion essentielles ou à des applications logicielles, qui sont souvent gérées par des fournisseurs indépendants. La téléphonie migre elle aussi vers les services en ligne en raison de l'augmentation du nombre d'entreprises qui choisissent les voix sur IP (VoIP) comme solution peu coûteuse par rapport à la téléphonie traditionnelle. À moins qu'elle n'ait été conçue de façon sécuritaire dès le début, une VoIP connectée à un réseau peut présenter une lacune en matière de sécurité dans un système pourtant sécuritaire.

# ANNEXE B
# MODÉLISATION DES RISQUES ET DES VULNÉRABILITÉS

Au cours des dernières décennies, les laboratoires nationaux et les assureurs privés aux États-Unis ont mis au point différentes méthodes pour mieux évaluer les risques et les vulnérabilités liés aux infrastructures essentielles en cas de menaces terroristes et de cyberattaques.

Aux États-Unis, le DHS a établi le National Infrastructure Simulation and Analysis Center (NISAC) pour élargir à l'échelle nationale les connaissances en matière de protection des infrastructures essentielles. Le NISAC a pour mission d'offrir des capacités de modélisation et de simulation aux fins d'analyse des risques et vulnérabilités liés aux infrastructures essentielles, et ce en prenant appui sur les travaux de recherche des laboratoires nationaux Sandia National Laboratories et Los Alamos National Laboratory[50].

Sandia Laboratories a mis au point une méthode pour évaluer les risques associés à différents types d'installations et d'infrastructures essentielles et pour les réduire en appliquant un processus visant à relever et à évaluer les mises à jour des systèmes de sécurité. Ce laboratoire a également collaboré avec la Environmental Protection Agency (EPA) et des groupes de l'industrie pour élaborer une méthode d'évaluation des risques qui permet d'évaluer la vulnérabilité des systèmes d'eau aux États-Unis. Parmi les outils possibles, mentionnons la modélisation fondée sur les agents, la modélisation cognitive et l'analyse des tendances idéologiques.

En partenariat avec le DHS, l'Argonne National Laboratory a établi une méthode permettant d'évaluer systématiquement la posture de sécurité et la vulnérabilité des infrastructures essentielles[51]. On évalue les vulnérabilités des secteurs et des sous-secteurs à l'aide d'un indice de la vulnérabilité dans le but de trouver des moyens possibles de réduire les vulnérabilités et d'aider à préparer les évaluations de risque sectorielles. Le propriétaire ou l'exploitant reçoit également une analyse des données recueillies pour une installation précise, ce qui donne une idée des forces et des faiblesses de celle-ci sur le plan de la sécurité. Cette initiative fait partie d'un vaste programme du DHS (Enhanced Critical Infrastructure Protection Program) visant à atténuer les vulnérabilités, à renforcer les relations et à améliorer l'échange d'information entre des organismes publics et privés.

AIR Worldwide, un cabinet américain de modélisation des risques en cas de catastrophe, a mis à jour son modèle lié au terrorisme pour les États-Unis en octobre 2011. Ce modèle s'adresse aux assureurs et aux réassureurs et vise à les aider à évaluer les pertes possibles en cas d'attentat terroriste. La base de données sur les cibles et les lieux d'intérêt d'AIR Worldwide englobe un éventail complet de cibles qui pourraient faire l'objet d'un attentat, dont bon nombre sont considérées comme des « cibles trophées ». On applique une méthode d'évaluation rigoureuse pour évaluer les éventuels attentats, tout en tenant compte d'un large éventail de menaces, y compris celles provenant d'extrémistes intérieurs, de régimes étrangers et d'organisations parrainées par des États, ainsi que des réseaux composés de petits groupes et d'individus partageant les mêmes idées[32].

Au Royaume-Uni, un intermédiaire renommé en matière de réassurance, Aon Benfield, a annoncé en novembre 2011 son nouveau « modèle pour les catastrophes liées au terrorisme au Royaume-Uni », comprenant des probabilités et des scénarios à jour. Ce modèle évalue les pertes financières pour le secteur de l'assurance-vie en cas d'attentat terroriste et contribue à satisfaire les exigences du projet de règlement de l'Union européenne Solvabilité II, qui oblige les assureurs à mieux comprendre les risques auxquels ils sont exposés et, par conséquent, leur stratégie d'achat de réassurance. Ce nouveau modèle simule des attentats contre des cibles possibles au Royaume-Uni, y compris des lieux de culte, des centres financiers, des infrastructures ainsi que des installations gouvernementales et militaires. Il tient compte des efforts déployés pour intégrer les évaluations réelles traditionnelles tout en tenant compte de la fréquence des incidents, des types d'attentats réalistes et des profils de dommages selon différents scénarios[33].

# NOTES EN FIN D'OUVRAGE

1 Voir annexe A et Lior Tabansky, « Critical Infrastructure Protection against Cyber Threats », *Military and Strategic Affairs*, vol. 3, n° 2, novembre 2011, p. 2.

2 États-Unis. National Research Council. *Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyber Attack Capabilities*, National Academies Press, 2009, p. 1.

3 Canada. Bureau du Conseil privé. *Protéger une société ouverte : la politique canadienne de sécurité nationale*, 2004. Sur Internet : http://www.bcp.gc.ca/docs/information/publications/aarchives/natsec-secnat/natsec-secnat-fra.pdf.

4 Canada. Sécurité publique Canada. *Stratégie nationale sur les infrastructures essentielles*, 2010. Sur Internet : http://www.securitepublique.gc.ca/prg/ns/ci/ntnl-fra.aspx.

5 Canada. Sécurité publique Canada. *Plan d'action sur les infrastructures essentielles*, 2010. Sur Internet : http://www.securitepublique.gc.ca/prg/ns/ci/_fl/ci-pln-fra.pdf.

6 Canada. Sécurité publique Canada. *Stratégie de cybersécurité du Canada : renforcer le Canada et accroître sa prospérité*, 2010. Sur Internet : http://www.securitepublique.gc.ca/prg/ns/cbrl_fl/ccss-scc-fra.pdf.

7 Toutefois, certaines organisations non gouvernementales et du secteur privé ne sont pas jugées comme faisant partie de l'infrastructure essentielle canadienne, comme les cabinets d'avocats, les sociétés de comptabilité générale, les organisations de recherche et de développement et les universités. Il est donc possible qu'elles possèdent des informations et des ressources documentaires d'importance nationale, mais elles ne seront peut-être pas consultées relativement à la cybersécurité dans le cadre des ententes de partenariat au titre de la Stratégie de cybersécurité du Canada.

8 Canada. Sécurité publique Canada. *Renforcer la résilience face au terrorisme*, Ottawa, 2012, p. 6-8.

9 *Ibid.*, p. 31-33.

10 *Ibid.*

11 Canada. Sécurité publique Canada. *Renforcer la résilience face au terrorisme*, Ottawa, 2012, p. 8.

12 *Ibid.*, p. 8.

13 *Ibid.*, p. 26-28.

14 Al-Qaïda en Arabie saoudite. *Excerpts from "The Laws of Targeting Petroleum-Related Interests"*, rédigé par le cheik Abdullah bin Nasser al-Rashid (alias Abdelaziz bin Rashid al-Anzi), Global Terror Alert, mars 2006. Sur Internet : www/globalterroralert.com.

15 Adeeb al-Bassam, « Bin Laden and the Oil Weapon », *Sawt al-Jihad* (Voix du djihad), mois de muharram, an 1428 de l'hégire (février 2007), p. 9. Paru dans « The Knight of Jihadi Media: Issa al-Awshan: A Special Interview with the Leader: Karim al-Majati - may Allah Accepts Him Bin Laden and the Oil Weapon », *Sawt al-Jihad* (Voix du djihad), n° 30, mois de muharram, an 1428 de l'hégire, traduit par le SITE Institute, Washington : « Al-Qaeda in Saudi Arabia Presents the Return of its Publication [Voice of Jihad], The Thirtieth Issue ».

16 Cheik Anouar al-Aulaki, « The Ruling on Dispossessing the disbelievers unbelievers; wealth in Dar al-Harb », *Inspire*, 1431/2010, p. 59.

17 « Full Transcript of bin Laden's Speech », *Al Jazeera.net*, 30 octobre, 2004. Sur Internet : http://english.aljazeera.net/NR/exeres/79C6AF22-98FB-4A1C-B21F-2BC36E87F61F.htm.

18 Canada. Sécurité publique Canada. *Renforcer la résilience face au terrorisme*, Ottawa, 2012, pp. 22-23.

19 Chef des Opérations à l'étranger, « The Objective of Operation Hemorrhage », *Inspire*, novembre 1341/2010, numéro spécial : « Operation Hemorrhage targeting air cargo aircraft », p. 7;
Yahya Ibrahim, « $4,200 », *Inspire*, novembre 1341/2010, numéro spécial : « Operation Hemorrhage targeting air cargo aircraft », p. 15.

20 Chef des Opérations à l'étranger, « The Objective of Operation Hemorrhage », *Inspire*, p. 7.

21 Yahya Ibrahim, « $4,200 », *Inspire*, p. 15.

22 Association France Presse, « Al-Qaeda calls for new attacks on the West », 25 février 2011.

23 United Kingdom, Secretary of State for the Home Department: *CONTEST. The United Kingdom's Strategy for Countering Terrorism* (London, July 2011), para. 2.47.

24 Mohammad Atayf, « Scholars speak out in favour of 'electronic Jihad' against the enemy », al-Arabiya online. Sur Internet : http://english.alarabiya.net/articles/2012/01/29/191307.html.

25 Gabriel Weimann, *WWW.Terror.Net. How Modern Terrorism Uses the Internet*, United States Institute of Peace, rapport spécial n° 116, mars 2004.

26 Diego Gambetta et Steffen Hertog, *Engineers of Jihad*, Département de sociologie, Université d'Oxford, Sociology Working Paper 2007-10m, pp. 8, 12.

27 États-Unis. National Research Council. *Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyber Attack Capabilities*, National Academies Press, 2009, p. 1.

28 États-Unis. Office of the President of the United States, *The Comprehensive National Cybersecurity Initiative*, Washington, 2008, mesure n° 3.

29 En 2011, 13 % des cyberattaques à l'échelle mondiale ont été attribuées au Myanmar : « Cyber War: Myanmar Leader in Cyber Attacks in 2011 », *Asia News*, 20 février 2011. Sur Internet : http://www.asianews.it/news-en/Cyber-war:-Myanmar-leader-in-attacks-in-2011-22224.html.

30 États-Unis. Département de la Sécurité intérieure, bulletin du National Cybersecurity and Communications Integration Center cité dans « DHS warns Anonymous may target critical infrastructure », *Cyber Security News Wire*, 4 novembre 2011. Sur Internet : http://www.homelandsecuritynewswire.com/dhs-warns-anonymous-may-target-critical-infrastructure.

31 Cité dans « DHS warns Anonymous may target critical infrastructure », *Cyber Security News Wire*, 4 novembre 2011. Sur Internet : http://www.homelandsecuritynewswire.com/dhs-warns-anonymous-may-target-critical-infrastructure.

32 Gary Davis, "2012 McAfee Threat Predictions: A look at the latest threats that could affect consumers this coming year," McAfee, December 27, 2011, accessible au: http://blogs.mcafee.com/consumer/2012-mcafee-threat-predictions-consumers.

33 Général Keith Alexander, directeur de la National Security Agency et chef du Cyber Command, cité par Jennifer Valentino-DeVries et Julia Angwin, « Defenses against Hackers are like the Maginot Line, says NSA Chief », *Wall Street Journal*, 14 janvier 2012.

34 Lisa Kramer et Richards Heuer Jr., « America's Increased Vulnerability to Insider Espionage », *International Journal of Intelligence and CounterIntelligence*, vol. 20, 2007.

35 Abou Bakr Naji, *Gestion de la barbarie*, Éditions de Paris, Versailles, 2007.

36 Nick Catrantzos, « No Dark Corners: A Different Answer to Insider Threats », *Homeland Security Affairs*, vol. 6, n° 2, mai 2010.

37 États-Unis. Département de la Sécurité intérieure, *Insider Threat to Utilities*, Washington, 19 juillet 2011. Sur Internet : http://info.publicintelligence.net/DHS-InsiderThreat.pdf. Voir aussi Brian Ross, Rhonda Schwartz et Megan Chuchmach, *New Terror Report Warns of Insider Threat to Utilities*, ABC News, 10 juillet 2011. Sur Internet : http://abcnews.go.com/Blotter/terror-alert-warns-insider-threat-infrastructure/story?id=14118119.

38 Symantec Corp. *Symantec Critical Infrastructure Protection Survey*, deuxième sondage annuel.

39 Brigid Grauman, *Cyber Security: The Vexed Question of Global Rule. An Independent Report on Cyber Preparedness Around the World* (Bruxelles : Security and Defence Agenda, 2012). Rapport rédigé avec l'aide de MacAfee Inc.

40 *Ibid.*, p. 8.

41 Pays-Bas, coordonnateur national de la lutte contre le terrorisme, *Technological Developments: Opportunities and Threats for Counterterrorism and Surveillance and Protection Until 2015*, publication I-8731 (n.d., 2011), p. 55.

42 Brigid Grauman, *Cyber Security: A Vexed Question of Global Rule. An Independent Report on Cyber Preparedness Around the World*, p. 58.

43 Nancy Hayden, « The Complexity of Terrorism: Social and Behavioral Understanding Trends for

the Future », *Information Age Warfare Quarterly*, vol. 1, n° 2, été 2006. Sur Internet : http://www.google.ca/search?q=%22Nancy+Hayden%22+%2B+wicked&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:en-US:official&client=firefox-a. Voir aussi Nancy Hayden, « The Complexity of Terrorism: Social and Behavioral Understanding » dans Magnus Ranstorp (sous la direction de), *Mapping Terrorism Research. State of the Art, Gaps, and Future Directions*, Routledge, Londres, 2007.

44 Symantec Corp. *Symantec Critical Infrastructure Protection Survey*, octobre 2011. Sur Internet : http://www.symantec.com/content/en/us/about/media/pdfs/symc_critical_infrastructure_protection_survey_2011.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2011Oct_worldwide_CIPSurvey.

45 États-Unis. Office of the President of the United States, *Trustworthy Cyberspace: Strategic Plan for the Federal Cyber security Research and Development Program*, Washington, décembre 2011. Sur Internet : http://www.whitehouse.gov/sites/default/files/microsites/ostp/fed_cybersecurity_rd_strategic_plan_2011.pdf.

46 Canada. Sécurité publique Canada. *Renforcer la résilience face au terrorisme*, Ottawa, 2012, pp. 22-23.

47 *Ibid.*, p. 17.

48 Brigid Grauman, *Cyber Security: A Vexed Question of Global Rule. An Independent Report on Cyber Preparedness Around the World*, pp. 43-44.

49 Intelligence and National Security Alliance (INSA). *Cyber Intelligence: Setting the Landscape for an Emerging Discipline*, septembre 2011, p. 3.

50 Le NISAC prépare et communique des analyses des infrastructures essentielles et des ressources clés, y compris les interdépendances, les vulnérabilités, les conséquences et les autres complexités, sous la direction de l'Office of Infrastructure Protection (IP), Infrastructure Analysis and Strategy Division (IASD). Pour assurer le respect des priorités d'IP, le bureau responsable du programme du NISAC coordonne les mesures auxquelles participe le Centre ainsi que les demandes qu'il reçoit.

51 William Buehring, Ronald Whitfield, Ronald Fisher et Michael Collins. « Protective measures and vulnerability indices for the Enhanced Critical Infrastructure Protection Programme », *International Journal of Critical Infrastructures*, vol. 7, n° 3, 2011. Sur Internet : http://www.inderscience.com/search/index.php?action=record&rec_id=42976&prevQuery=&ps=10&m=or.

52 Air Worldwide. « Terrorism ». Sur Internet : http://www.air-worldwide.com/terrorism.aspx; « Assessing Terrorism Risk Ten Years After 9/11 ». Sur Internet : http://www.air-worldwide.com/PublicationsItem.aspx?id=21161.

53 Communiqué de presse – Aon Benfield, 14 novembre 2011, « Aon Benfield launches UK terrorism catastrophe model with updated attack scenarios and probabilities ». Sur Internet : http://aon.mediaroom.com/index.php?s=43&item=2481.